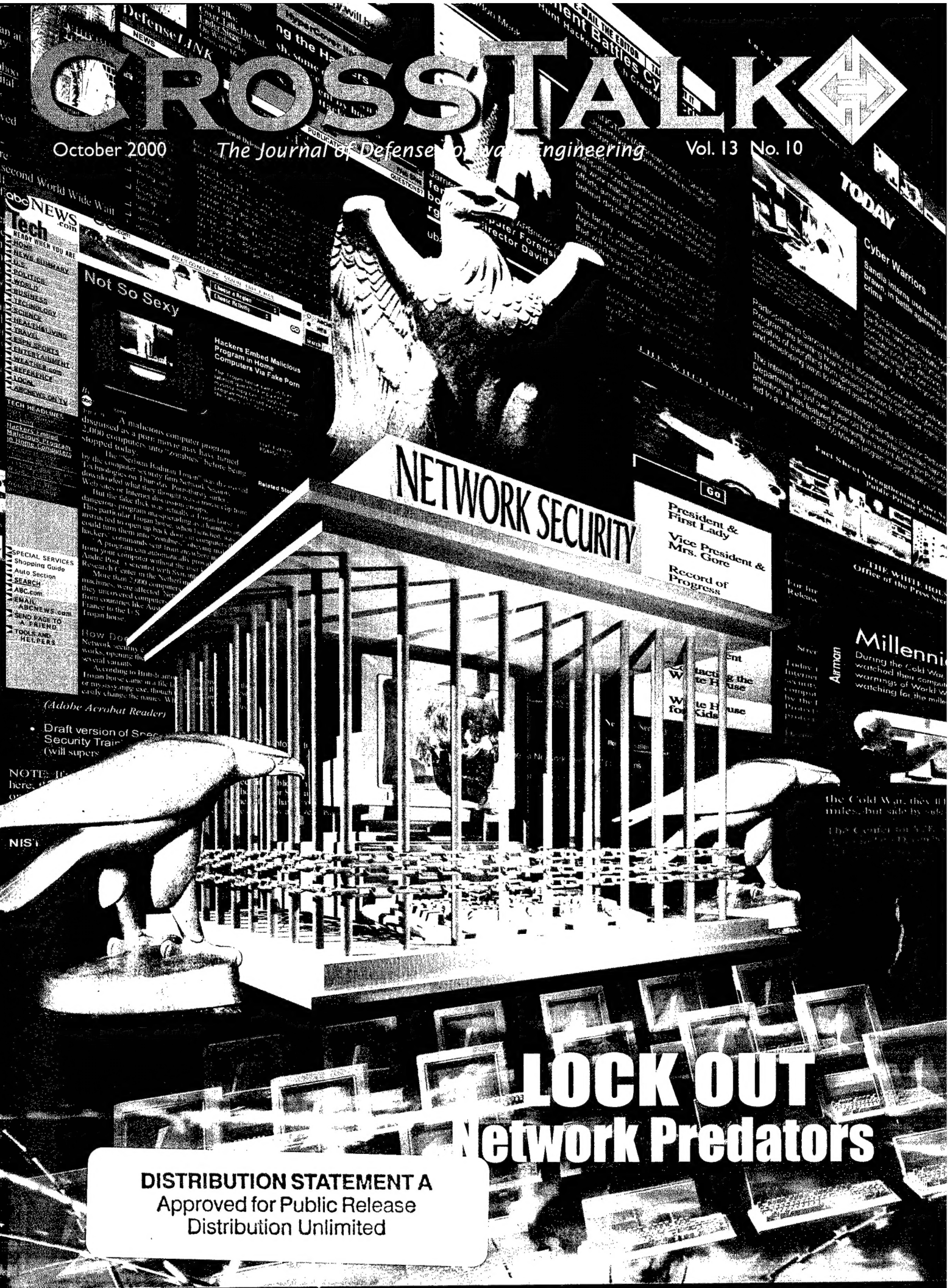
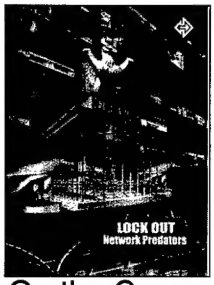

CROSSTALK
October 2000
The Journal of Defense Software Engineering
Vol. 13 No. 10
NETWORK SECURITY
Not So Sexy
Hackers Embed Malicious Program in Home Computers Via Fake Porn
TODAY
Cyber Warriors
President & First Lady
Vice President & Mrs. Gore
Record of Progress
LOCK OUT
Network Predators
DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Network Security



On the Cover: Kent Bingham, Digital Illustration and Design, is a self-taught graphic artist/designer and freelances both print and Web design projects. His portfolio is at www.adobe.com/eportfolio/kentbingham

Open Forum

Software Engineering Technology

wi crossed es

The author of *Don't Say the 'P' Word,* Lori Pajerek, was incorrectly identified in the August table of contents. CROSSTALK regrets the error.

Departments

CROSSTALK

Sponsor *Lt. Col. Glenn A. Palmer*

Publisher *Reuel S. Alder*

Managing Editor *Pam Bowers*

Associate Editor/Layout *Matthew Welker*

Associate Editor/Features *Heather Winward*

Graphic Design *Abby Hall*

Voice 801-586-0095
Fax 801-777-5633
E-mail crosstalk.staff@hill.af.mil
STSC Online www.stsc.hill.af.mil
CrossTalk Online www.stsc.hill.af.mil/Crosstalk/crostalk.html
CRSIP Online www.crsip.hill.af.mil

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address. You may use the form on page 31.

Ogden ALC/TISE
5851 F Ave.
Bldg. 849, Rm. B-04
Hill AFB, Utah 84056-5713

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CROSSTALK editorial board prior to publication. Please follow the ***Guidelines for CROSSTALK Authors,*** available upon request. We do not pay for submissions. Articles published in CROSSTALK remain the property of the authors and may be submitted to other publications.

Reprints and Permissions: Requests for reprints must be requested from the author or the copyright holder. Please coordinate your request with CROSSTALK.

Trademarks and Endorsements: This DoD journal is an authorized publication for members of the Department of Defense. Contents of CROSSTALK are not necessarily the official views of, or endorsed by, the government, the Department of Defense, or the Software Technology Support Center. All product names referenced in this issue are trademarks of their companies.

Coming Events: We often list conferences, seminars, symposiums, etc., that are of interest to our readers. There is no fee for this service, but we must receive the information at least 90 days before registration. Send an announcement to the CROSSTALK Editorial Department.

STSC Online Services: at www.stsc.hill.af.mil. Call 801-777-7026, e-mail: randy.schreifels@hill.af.mil.

Back Issues Available: The STSC sometimes has extra copies of back issues of CROSSTALK available free of charge.

The Software Technology Support Center was established at Ogden Air Logistics Center (AFMC) by Headquarters U.S. Air Force to help Air Force software organizations identify, evaluate, and adopt technologies to improve the quality of their software products, efficiency in producing them, and their ability to accurately predict the cost and schedule of their delivery.

You Cannot Pass the Buck on Reliable Network Security

Who has the responsibility within your organization to ensure that the network everyone has come to rely upon stays operational? Typically, you may respond: "Oh, that is taken care of by our network administrator. They stay on top of that. That is why we pay them the *big bucks!*" Unfortunately, as we learn from Moira West-Brown in *Avoiding the Trial-by Fire Approach to Security Incidents,* "Most organizations do not even think of how to respond to a computer security incident until after they have experienced a significant one."

Most of us probably do not care to know what is being done to keep our networks up until we are affected personally. How many of us were *not* impacted in some way by the recent Love Letter e-mail virus attack? West-Brown also points out that insurance coverage for security losses will likely be changing. Some insurance companies offer financial protection for third-party damages resulting from security breaches. However, she says, "It is only a matter of time before insurance companies begin to request more information about network security, and begin to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer-security incidents."

Networks have become indispensable for conducting business everywhere—in government, industry, and your organization. Networked systems allow access to needed information rapidly, improving communications while reducing costs. This reduction in costs, however, could be easily overshadowed by the cost of security breaches as indicated in *Improving the Security of Networked Systems,* by Julia Allen, et al. They note that security breaches are on the rise, and the cost is increasing. Financial losses for reporting organizations have doubled to more than $265 million according to a recent survey. Is your organization at risk? How would you know? Read this article and discover that the goal of OCTAVE[SM] [1] is "to improve how well information assets are protected, putting organizations in a better position to achieve their missions." OCTAVE enables organizations to develop appropriate protection strategies by considering policy, management, administration, and other organizational issues, as well as technologies, to form a comprehensive view of the information security state of that organization.

Another method providing a systematic means to assess and improve system survivability for risk reduction is described in *The Survivability Imperative: Protecting Critical Systems* by several authors of the Software Engineering Institute. Our modern society is increasingly dependent upon complex network environments. Complex systems may improve efficiency, but they also introduce additional intrusion risks by unknown parties with destructive motivations. These risks can be mitigated by incorporating survivability capabilities, according to the authors. "Survivability analysis is a prudent risk management technique in a world that increasingly depends on complex, large-scale network systems," they conclude.

An interesting perspective on some of the challenges we face in taking full advantage of the electronic capabilities to streamline government and consumer/customer service is outlined in *Electronic Commerce and Governance: A Darwinian Discussion* by Nancy Lee Hutchin. She addresses learning to deal with removing personal feedback in online service relationships. How much are we willing to trust someone we cannot look in the eye? How do we evaluate trustworthiness? Are we willing to change the way we do business for time savings or convenience?

Several of this month's articles also mention the use of best practices as outlined in one of the Capability Maturity Models (CMMs). In *Avoid Self-Inflicted Wounds in Applying CMM to ATP Maintenance and Support,* David Putman discusses how to apply CMM concepts to hardware and software engineering. Rick Hefner, Ron Knode and Mary Schanken's article *The Systems Security Engineering CMM* describes essential characteristics of an organization's process required for good security engineering. In her article, Hutchin highlights the quantifiable business benefits achievable in moving from CMM level one to CMM level three. As a member of the CMM integrated product development team for more than two years, I enthusiastically recommend your continued interest in use of CMMs in all of your information technology process improvement efforts. I hope this month's issue of CROSSTALK will provide several new ideas to benefit your organization.

H. Bruce Allgood
Deputy Computer Resources Support Improvement Program Director

1. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a service mark of Carnegie Mellon University.

The Systems Security Engineering CMM

Rick Hefner
TRW

Ron Knode
Computer Sciences Corp.

Mary Schanken
National Security Agency (NSA)

The Systems Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The model also highlights the relationship between security engineering and systems engineering. This article discusses how the security community is applying the SSE-CMM to help solve today's security issues. These include leading contractors improving their practices, acquisition agencies evaluating potential system security vendors, and potentially using the model as an international standard.

A CMM® is a reference model of mature practices for a specified engineering discipline. A project developer or organization can compare practices to the model to identify potential improvements. Many companies have used CMMs to improve their software and systems engineering practices [1, 2].

The field of security engineering has several well-accepted criteria for evaluating security products, systems, and services [3, 4, 5, 6]. However, it lacks a comprehensive framework for evaluating security engineering practices. The SSE-CMM provides a way to measure and improve capability in applying security engineering principles, and to address capability-based assurance.

Project History

The NSA initiated development of the SSE-CMM to foster improvement in the security engineering process and to augment existing assurance methods. In 1995 the agency formed a government-industry consortium with wide representation from the security engineering acquisition and supplier communities. Organizations that provide or acquire security engineering systems, products, or services were encouraged to participate. The agency also invited identified experts in the security engineering community to review and comment on project materials.

Model and Appraisal Method

The SSE-CMM identifies both the unique characteristics of security engineering, and the integration of security activities into the overall system engineering process. The SSE-CMM uses the same maturity model architecture used in the System Engineering (SE)-CMM [2].

SSE-CMM Project Participants

- Arca Systems Inc.
- BDM International Inc.
- Booz-Allen and Hamilton Inc.
- Communications Security Establishment (Canada)
- Computer Sciences Canada
- Computer Sciences Corp.
- Data Systems Analysts Inc.
- Defense Information Systems Agency
- E-Systems
- Electronic Warfare Associates - Canada, Ltd.
- Fuentez Systems Concepts Inc.
- G-J Consulting
- GRC International Inc.
- Harris Corp.
- Hughes Aircraft
- Institute for Computer and Information Sciences
- Institute for Defense Analyses
- Internal Revenue Service
- ITT
- Lockheed Martin
- Merdan Group Inc.
- MITRE Corp.
- Motorola
- National Center for Supercomputing Applications, Univ. of Illinois
- National Security Agency
- National Institute for Standards and Technology
- Naval Research Laboratory
- Navy Command, Control, Operations Support Center Research, Development, Testing and Evaluation Division
- Northrop Grumman
- Office of the Secretary of Defense
- Oracle Corporation
- pragma Systems Corporation
- San Antonio Air Logistics Center
- Science Applications International Corp.
- SPARTA Inc.
- Stanford Telecom
- Systems Research and Applications
- Tax Modernization Institute
- The Sachs Groups
- tOmega Engineering
- Trusted Information Systems
- TRW
- Unisys Government Systems

Model Structure

The model is divided into two dimensions: domain and capability. On the domain side [Figure 1], practices are organized in a hierarchy of process categories, process areas, and base practices. The SSE-CMM augments project and organizational process areas from the SE-CMM with security-specific process areas, including:

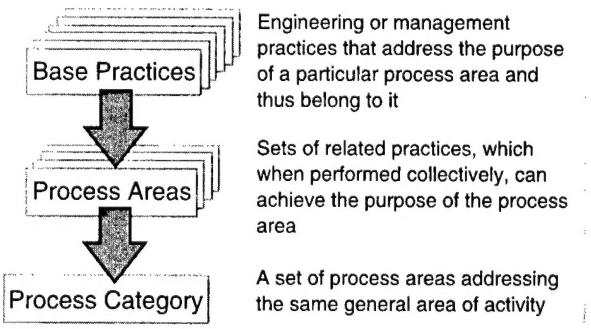
- Administer Security Controls.
- Assess Impact.
- Assess Security Risk.
- Assess Threat.
- Assess Vulnerability.
- Build Assurance Argument.
- Coordinate Security.
- Monitor Security Posture.
- Provide Security Input.
- Specify Security Needs.
- Verify and Validate Security.

On the capability side (Figure 2), the model identifies capability levels from zero to five. Higher levels imply increased organizational support for planning, tracking, training, etc., which leads to more consistent performance of the domain activities. This support is captured in a set of common features and generic practices for each level. Further details are in [7].

SSE-CMM Pilots

The SSE-CMM is structured to support a wide variety of

Figure 1. *Domain Aspect*



® The Capability Maturity Model and CMM are registered service marks of the Software Engineering Instutute and Carnegie Mellon University.

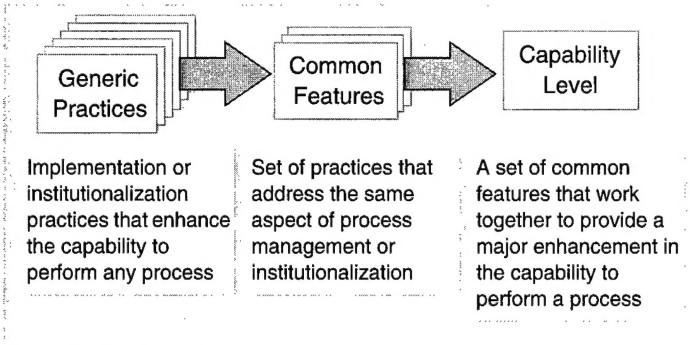


Figure 2. *Capability Aspect*

improvement activities, including self-administered appraisals or internal appraisals augmented by expert facilitators from inside or outside the organization. Although it is primarily intended for internal process improvement, it can also be used to evaluate a potential vendor's capability to perform its systems security engineering process.

An assessment against this model involves determining the appropriate capability level for each process area. To determine appropriate improvement actions, the organization must decide what capability they desire in each of the process areas, and address any deficiencies. An appraisal methodology, termed the System Security Appraisal Method (SSAM), was defined [8].

The purpose of the SSE-CMM pilot program [9], conducted during 1996, was to validate the model and appraisal method, focusing on the Security Engineering Process Areas (PAs). The pilots were performed under nondisclosure agreements with the host organizations, covering proprietary process information and assessment results.

Because the SSAM is based on the SE-CMM Assessment Method, pilot team members received training on the SE-CMM assessment method and adapted it for the SSE-CMM. Since some organizations will want to perform a SSE-CMM assessment in conjunction with a SE-CMM assessment, the Security Appraisal Method was revised to shorten the typical assessment duration.

This was accomplished by redesigning the questionnaire, streamlining the questionnaire analysis process, eliminating redundant data entry, and increasing the emphasis on pre-onsite activities. According to pilot participants with SE-CMM assessment experience, these changes did not detract in any way from the quality and accuracy of the assessment.

TRW, a major integrator of secure systems, hosted the first pilot appraisal. The appraisal focused on a single project—a system integration effort covering the life cycle from concept to system delivery, including concept definition, definition and analysis of requirements, design, analysis, implementation, and testing. The appraisal addressed the following Process Areas:

- Assess Operational Security Risk.
- Attack Security.
- Build Assurance Argument.
- Coordinate Security.
- Determine Security Vulnerabilities.
- Provide Security Input.
- Specify Security Needs.
- Verify and Validate Security.

The second pilot focused on security service projects, specifically risk analyses and assessments at Computer Sciences Corp. The appraisal covered two projects: a system in development and an operational system. The engineering PAs addressed were the same as the first pilot with the addition of Adminster Security Controls and the deletion of Provide Security Input.

The remaining three pilots were hosted by Hughes (another system integrator), GTIS (a certification authority), and Data General (a product vendor). The pilots uncovered some potential improvement areas, and the model and appraisal method were updated.

Model Applications Best Operational Practice

One interesting application of the SSE-CMM involves the selection of base practices as identified within selected PAs and forming them into policy statements, process handbooks, or procedural instructions for a specific organization. One of the most notable uses of the SSE-CMM in this manner is the generation of a Model Information System Security Program (MISSP) under the U.S. Agency for International Development (USAID).

The MISSP consists of a framework that links and categorizes collections of best practices that cover an entire information security program. It is intended to be used by any civil government agency that needs to generate a comprehensive information security program, but which may not have the time or resources to start from scratch. NSA, the Critical Infrastructure Assurance Office, and the Federal Chief Information Officer Council endorse the MISSP concept.

In late 1999, the U.S. Federal Chief Information Officer Council adopted the USAID MISSP as the foundation for a collection of Best Security Practices.

Standard for Performance

The SSE-CMM is increasingly being viewed as the process analog to the product metric presented by the *Common Criteria* and the National Information Assurance Partnership. For example, the *Common Criteria* is being used to generate protection profiles for the components of a Public Key Infrastructure (PKI) to be deployed throughout the Department of Defense (DoD). The protection profiles will then represent the security requirements that need to be present—and evaluated—in vendor equipment being used within this DoD PKI.

The SSE-CMM is being researched as the source for the process equivalent of protection profiles for this same purpose. That is, the SSE-CMM will be used to prepare capability profiles that will describe the organizational security capability requirements for the design, development, deployment, and operation of this PKI within the DoD. If such capability profiles emerge, then the SSE-CMM appraisal method would also be used to verify the existence of such capabilities. This works in the same way a *Common Criteria* evaluation under the National Information Assurance Partnership verifies the existence of security features and assurances in the products being used.

Another use of capability profiles is to include them as a portion of the metrics identified within Service Level Agreements (SLAs) in outsourcing contracts. In this circumstance, periodic appraisals of performing organizations will con-

tribute to the scoring of information security service delivery in accordance with the SLAs. It will ultimately help determine the payment for services rendered.

NSA used the SSE-CMM in the development of an Industrial Information Systems Security Engineering (ISSE) Certification Program to help customers of ISSE services identify qualified ISSE Service Providers and to raise the quality of the service provided throughout the community.

NSA is currently using two tailored versions of the SSE-CMM: the Information Security (INFOSEC) Assessment CMM (IACMM) and the Business CMM (BCMM). The IACMM was designed to measure the capability of an INFOSEC assessment organization. The purpose is to help build a cadre of INFOSEC assessor organizations that are well equipped to provide valid site assessments to their customer base. This will help alleviate the huge demand for NSA resources to conduct such assessments by providing a standardized metric that customers can use to measure the capabilities of suppliers to address the specific INFOSEC assessment needs.

The BCMM was developed in order to measure the Information Systems Security Organization's Business Health. The focus is on the supporting business processes that any organization relies upon to ensure appropriate and timely execution of its mission objectives (i.e. Product and/or Service-based.) At the time of this writing, three pilot appraisals and eight BETA appraisals have been conducted.

Under the National Information Assurance Partnership, NSA has used the SSE-CMM to capture process-related security awareness activities that are included in the National Institute of Standards and Technology National Voluntary Laboratory Accreditation Program Handbook 150-20: *Information Technology Security Testing—Common Criteria.* The inclusion of this set of queries closes the gap between product and process assurance issues in the Common Criteria lab accreditation program.

The SSE-CMM has been submitted to the International Organization for Standardization as a Publicly Available Specification. NSA is also working to have the security Process Areas of the SSE-CMM included in the SEI CMM Integration (CMMI[SM]) initiative.

The Canadian Security Establishment (CSE) stated it is considering using the SSE-CMM to:

- Perform an internal appraisal within Computer and System Security Section of CSE.
- Encourage product vendors to use it to become more mature, helping them to develop better products and facilitate evaluation process.

Conclusion

This paper summarizes the development, piloting, and use of the SSE-CMM. Obviously, there is much to do before the SSE-CMM is fully integrated and in widespread use throughout the security community.

The SSE-CMM must further explore the relationship among current approaches to assurance. The current product-based approach relies on identifying a series of criteria that are evaluated for each intended product or system, based on the intended operating environment and the perceived threats therein.

As the number and variety of secure systems and products increases, and operating environments and security threats become increasingly diverse, this approach is becoming costlier. Customers are looking to developmental assurance methods, such as the SSE-CMM, to reduce the extent that product-based criteria are used, and to reduce the evaluation and accreditation time. This highlights three aspects of security protection:

- Product (e.g., common criteria).
- Process (e.g., organizaional capability via the SSE-CMM).
- Pedigree (e.g., personal capability via the Certified Information Systems Security Professional exam).

Based on the successful results to date and the current initiatives, we expect that use of the SSE-CMM will increase dramatically in the next few years, until the model becomes an industry standard. Only then will the benefits of this model be fully seen.◆

References

1. Paulk, Mark; Curtis, William; and Chrissis, Mary Beth, *Capability Maturity Model for Software, Version 1.1,* Software Engineering Institute, CMU/SEI-93-TR-24, DTIC # ADA263403, February 1993.
2. Bates, Roger, et al, *A Systems Engineering Capability Maturity Model, Version 1.1.* CMU/SEI-95-MM-003, November 1995.
3. *Department of Defense Trusted System Evaluation Criteria,* DOD 5200.28-STD, December 1985.
4. *Common Criteria for Information Technology Security Evaluation,* Version 2.1, CCIMB-99-031, August 1999.
5. *The Specification for Information Security Management Systems,* BS 7799: Part 2, February 1998.
6. *DoD Information Technology Security Certification and Accreditation Process (DITSCAP),* DoDI 5200.40, Dec. 30, 1997.
7. SSE-CMM Project, *Systems Security Engineering Capability Maturity Model, Version 1.0,* Apr. 1, 1999.
8. SSE-CMM Project, *Systems Security Appraisal Method, Version 1.0,* Oct. 21 1996.
9. Hefner, Rick; Monroe, Warren; and Hsaio, David, *Experience with the Systems Security Engineering Capability Maturity Model,* Proceedings of the Sixth Annual International Symposium of the National Council of Systems Engineering, Boston, Mass., July 7-11, 1996.

About the Authors

Rick Hefner, Ph.D., is the manager of Process Technology for TRW. He has more than 25 years of experience in software development, research, and management, and has worked in industrial, academic, and government positions. He is co-chairman of the Assessment Methodology Team on the CMM integration project. He is an SEI-authorized lead assessor, and has published more than 30 papers. He received his bachelor of science degree and master of science degree from Purdue University and his doctorate degree from UCLA.

One Space Park
Redondo Beach, Calif. 90278
Voice: 310-812-7290
Fax: 310-8121251
E-mail: rick.hefner@trw.com

See page 25 for biographies of Ron Knode, Mary Schanken.

Improving the Security of Networked Systems

By Julia Allen, Christopher Alberts, Sandi Behrens, Barbara Laswell, and William Wilson
Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University

As the Internet and other national information infrastructures become larger, more complex, and more interdependent, the frequency and severity of unauthorized intrusions is increasing. Therefore, to the extent possible and practical, it is critical to secure the networked systems of an organization that are connected to public networks. This article describes an emerging approach and set of activities for establishing and maintaining the security of networked systems.

Targeting the Problem

Networks have become indispensable for conducting business in government, industry, and academic organizations. Networked systems allow access to needed information rapidly, improve communications while reducing costs, enable collaboration with partners, provide better customer services, and conduct electronic commerce [1].

Organizations have moved to distributed, client-server architectures where servers and workstations communicate through networks. In addition, they are connecting their networks to the Internet to sustain a visible business presence with customers, partners, and suppliers. While computer networks revolutionize the way business is done, the risks they introduce can be fatal. Attacks on networks can lead to lost money, time, products, reputation, sensitive information, and even lives.

The *2000 Computer Security Institute/FBI Computer Crime and Security Survey* [2] indicates that computer crime and other information security breaches are still on the rise, and the cost is increasing. For example, 70 percent of the 585 respondents reported computer security breaches within the last twelve months, up from 62 percent in 1999. Furthermore, the financial losses for the 273 organizations that could quantify them totaled $265,586,240, a 100 percent increase over the $123,779,000 reported in 1999.

Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people to perform their work more effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap between the knowledge needed to operate a system and that needed to keep it secure leads to increasing numbers of vulnerable systems [3].

Technology evolves so rapidly that vendors concentrate on time-to-market, often minimizing that time by placing a low priority on security features. Until customers demand products that are more secure, the situation is unlikely to change.

Users count on their systems being there when they need them, assuming that their information technology (IT) departments are operating all systems securely. This may not be the case. System and network administrators typically have insufficient time, knowledge, and skill to address the wide range of demands to keep today's complex systems and networks up and running. Additionally, evolving attack methods and software vulnerabilities continually introduce new threats to an organization's installed technology and systems. Thus, even vigilant, security-conscious organizations discover that security starts to degrade almost immediately after fixes, workarounds, and newly installed technology are put in place.

Inadequate security in the IT infrastructures can negatively affect the integrity, confidentiality, and availability of systems and data.

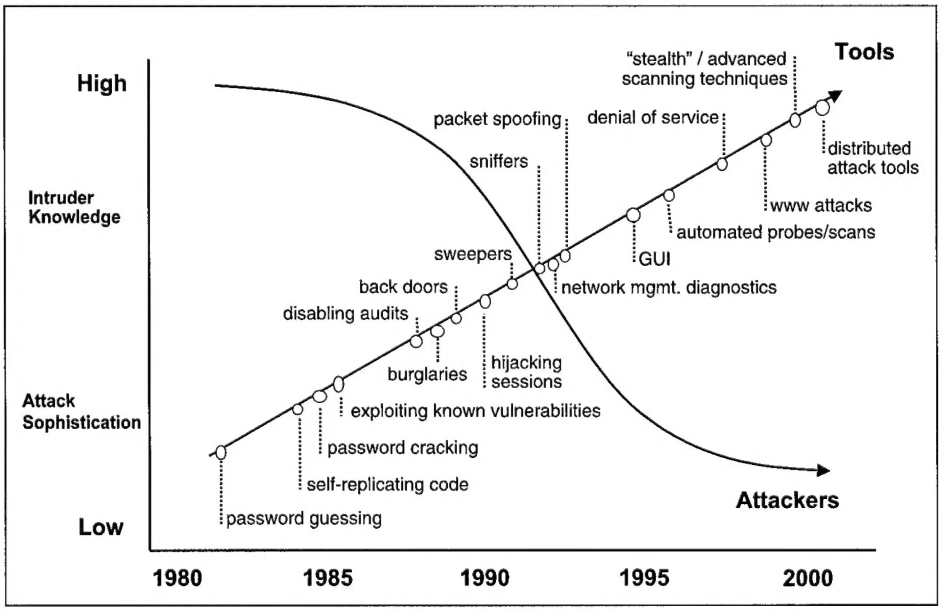
Who has this problem? The answer is just about everyone—anyone that uses information technology infrastructures that are networked, distributed, and heterogeneous needs to care about improving the security of networked systems.

Why Improve Security?

Why should you care about this problem? Whether you acknowledge it or not, your organization's networks and systems are vulnerable to attack by both insiders and outsiders. Organizations cannot conduct business and build products without a robust IT infrastructure. In addition, users have an organizational and ethical responsibility to protect competitive and sensitive information. They must also preserve the reputation and image of their organizations and business partners. All of these can be severely compromised by successful intrusions.

In the 1980s intruders were the sys-

Figure 1. *Attack Sophistication vs. Intruder Technical Knowledge*



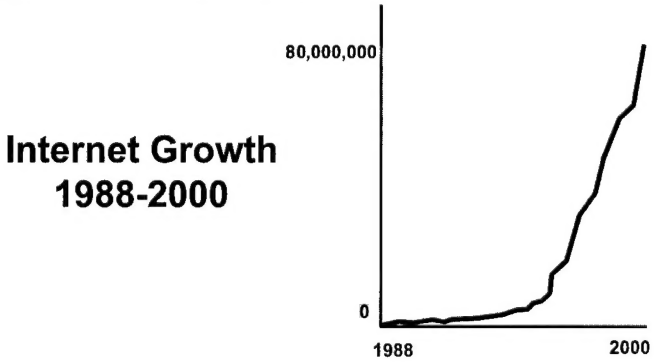
tem experts, as depicted in Figure 1. They had a high level of expertise and personally constructed methods for breaking into systems. Automated tools and exploit scripts were the exception rather than the rule. Today, absolutely anyone can attack a network due to the widespread and easy availability of intrusion tools and exploit scripts that can easily duplicate known methods of attack. While experienced intruders are getting smarter—as demonstrated by the increased sophistication in the types of attacks—the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing. Meanwhile, as evidenced by distributed denial-of-service attacks and variants of the Love Letter Worm, the severity and scope of attack methods is increasing.

In the early to mid-1980s, intruders manually entering commands on their personal computers could access tens to hundreds of systems; today, intruders use automated tools to access thousands to tens of thousands of systems. In the 1980s, it was relatively straightforward to determine if an intruder had penetrated your systems, and discover what they did. Today, intruders are able to totally hide their presence, for example, by disabling commonly used services and reinstalling their own versions, then erasing their tracks in audit and log files. In the 1980s and early 1990s, denial-of-service attacks were infrequent and not considered serious. Today, for organizations such as Internet service providers that conduct business electronically, a successful denial-of-service attack can put them out of business. Unfortunately, these types of attacks occur more frequently each year.

Due to exploding Internet use the demand for individuals with necessary technical education far exceeds the supply required to meet the need (see Figures 2 and 3). This is true for both those in formal degree programs and those who have acquired on-the-job knowledge and skills. As a result, people who are not properly qualified are being hired or promoted from within to do the job. This trend is exacerbated by the fact that some skilled, experienced system administrators change jobs frequently to increase their salaries or leave the job market because of burnout.

Today's audit and evaluation products typically focus on the underlying system and network technologies without considering the organizational concerns (e.g., policies, procedures) and human aspects (e.g., management, culture, knowledge and skills, incentives) that can dramatically affect the security posture of IT infrastructures. As a result, incomplete or point solutions are implemented with the expectation that they will completely solve the problem.

Figure 2. *Internet Growth by Number of Hosts*



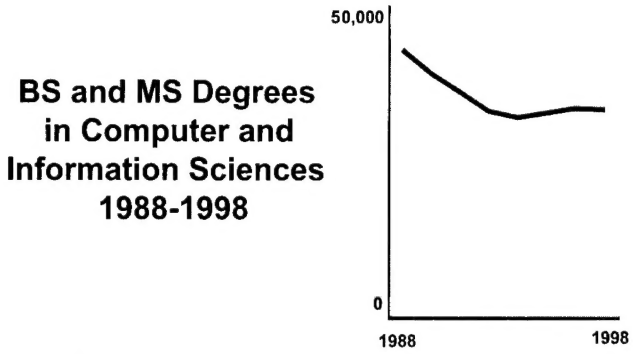


Figure 3. *Degrees in Computer and Information Sciences from 1988 to 1998*

The Meaning of Improved Security

Improving security is hard work, even if you have had a significant attack that has gotten everyone's attention. Sustaining a desired level of security can be even harder. First, you need to identify the risks to your business if the security (confidentiality, availability, and integrity) of critical data, systems, and/or networks (assets) is compromised. By compromised, we mean that the asset has been destroyed, damaged, or altered in a way that hurts your operations, or has been revealed to your competitors.

You cannot protect everything equally, so it is important to carefully choose the data you want to protect and then plan how to do so based on its value to your organization [4].

Once you know the risks to your networked system, you need to decide which ones are most likely to occur and which would cause the largest potential impact. The impact could be measured in money, time, lost productivity, or loss of market share, customers, or reputation. After deciding on a prioritized list of risks and an effective plan to mitigate them, there is still work to be done.

Suppose that a day after you create your plan, you find out that your main competitor has just launched a new e-commerce site and is ready to do business on the Internet—and you are still six months away from launching yours. Or suppose a recently fired employee has successfully penetrated your strategic planning database and posted your plans for the next 18 months on an Internet newsgroup. In other words, change and surprises introduce new risks that must be added to the ones you are already managing.

Since the technology and business environment is highly dynamic, an organization needs mechanisms for identifying critical information assets as conditions change. You need to have a way of adjusting where you invest time and energy for improving security based on this very dynamic environment.

Information Security Risk Assessment

Information protection decisions are often incomplete or ineffective because they are based on the organization's prior experience with vulnerabilities and current threats. While managing information security risks helps ensure that information protection strategies are appropriate, most risk assessments are incomplete, or are conducted by external consultants who have little knowledge of the organization's unique requirements. In order to address the widening gap between current risk management practice and the need for flexible, effective information protection, the Networked Systems Survivability (NSS) Program at

the Software Engineering Institute (SEI) is developing a comprehensive, repeatable technique for identifying vulnerabilities in networked systems through organizational self-assessment.

This self-assessment, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE℠)[1] [5], enables organizations to develop appropriate protection strategies by considering policy, management, administration, and other organizational issues, as well as technologies, to form a comprehensive view of the information security state of that organization. This method is a key component of an overarching security and information protection framework that allows an organization to identify and pursue an appropriate security posture.

An effective risk management strategy requires more than an assessment of the existing information infrastructure. An organization needs to understand:

- Value of the assets that must be protected.
- Consequences of loss of confidentiality or operational capability.
- Vulnerabilities that could be exploited to bring about the losses.
- Existing threats that could exploit the vulnerabilities.
- Likelihood that a threat might occur.
- Availability and appropriateness of options and resources to address risks and concerns.

The OCTAVE method is composed of three phases that provide a systematic, context-driven approach to managing information security risks, and enables an organization to assemble a comprehensive picture of their information security needs. Phase 1 identifies information assets and their values, as well as threats to those assets and the security requirements to protect them. This is accomplished using staff knowledge from multiple levels within the organization along with standard catalogs of information. This information can then be used to achieve the Phase 1 goal, which is to establish the security requirements of the enterprise.

Phase 2 examines the information assets of the organization in relation to the information infrastructure components to identify those components that are high priority. Then, staff evaluates the vulnerabilities within the infrastructure. At the conclusion of Phase 2, the organization has identified the high-priority information infrastructure components, missing policies and practices, and vulnerabilities.

Phase 3 builds on the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities. Estimates of impact and probability of the risks are made, and the risks are then prioritized, ultimately resulting in the development of a protection strategy and a comprehensive, enterprise-wide plan for managing information security risks.

OCTAVE has many unique features that extend its impact far beyond a comprehensive risk assessment. First, OCTAVE provides an organizing framework as well as a method that capitalizes on the abilities, practices, and mission of the organization performing the self-assessment. Thus, it helps organizations understand what current strategies and practices are working effectively. It also reveals needed improvements and gaps existing in strategy, technology, staff knowledge, and in the organization's ability to protect key information assets in a constantly changing environment.

Second, OCTAVE requires effective communication among all levels of staff and management. This is one of the long-lasting benefits.

Third, OCTAVE helps provide a clear picture of gaps in internal capabilities, thus enabling a strategy to be built that can include appropriate use of specialized, external experts. Ultimately the goal of OCTAVE is to improve how well information assets are protected, thus putting organizations in a better position to achieve their missions.

Inherent in the OCTAVE method is the assumption that an organization is already working to meet its mission objectives by using many good protection strategies. There are many practices that are commonplace; some are effective and some are not. The NSS Program continues to define technology and management practices that provide practical guidance, which will help organizations address important problems in network security.

Recommended Security Practices

One of the most important parts of adopting recommended security practices is selecting those that will allow you to mitigate your most critical technical risks. When considering who could most benefit from pragmatic, concise, how-to guidance about security (practices), it became obvious that the audiences with the greatest need were network and system administrators and their managers. They face the most daunting challenges as a result of the growth and complexity of their IT infrastructures, which they must keep in operation around the clock, seven days a week. They are constantly being asked to add new IT systems, networks, applications, and data to keep pace with changing business and technology demands.

Based on the actions successful organizations were taking to deal with these demands, the NSS program has developed step-by-step guidance that does not rely on a particular operating system or platform. The intent was to make the information as useful as possible. In addition, the NSS program developed UNIX- and Windows NT-specific implementations for many of the practices. All of this information can be found at the CERT® Coordination Center[2] (CERT/CC) Web site on the security improvement page.[3]

Each practice contains:

- A brief description that expands the title of the practice.
- An explanation of why the practice is important (what casualties can occur if you do not implement the practice).
- A step-by-step description of how to perform the practice.
- A collection of related policy topics that support deploying the practice successfully.

As data becomes available from organizations implementing recommended security practices, the practices will also provide:

- The cost/benefit analysis information for selecting among alternative approaches, and
- The means to measure implementation success (did it solve the problem it purported to solve, and were the benefits of the investment worth the cost?).

Some of the more frequently referenced sets of practices (each set is called a module) include Preparing to Detect Signs of Intrusion, Detecting Signs of Intrusion, Responding to

Intrusions, Securing Desktop Workstations, Securing Network Servers, Securing Public Web Servers, and Deploying Firewalls. The modules contain practices such as:

- Establishing requirements, policies, and procedures.
- Establishing secure architectures and configurations.
- Identifying and installing tools.
- Setting up logging options, examining what they produce.
- Setting up user authentication and file access control mechanisms.
- Determining how to deny network traffic that you do not want coming into your system.

Many of the practices are starting to appear in training materials and are being referenced by other web sites.

Curriculum and Certification Standards

Information systems security training at the SEI uses a variety of source material and experience in developing courses, including recommended practices and implementations. Relevant data from CERT/CC incident response and vulnerability analysis operations are used to provide current information on trends and emerging threats. CERT/CC experience in helping to foster the creation of other incident response teams around the world provides the core content for the suite of incident handling courses [6]. Research in the areas of security risk management and information survivability similarly provide core content for course development.

Comprehensive solutions for the survivability of information systems require that senior executives and managers, as well as technical staff, develop strong and diverse skills. Senior management must establish a clear sense of priority levels and appropriate policies, as well as risk-mitigation strategies, for securing various information assets. They share this guidance with technical staff responsible for the secure administration of networked systems. The first-line managers of technical staff must be able to articulate the technical implications of these decisions so cost-benefit tradeoffs can be performed.

The NSS program is in the process of developing security curricula for managers and system administrators. As a result of course development in the areas of Internet security, e.g. incident handling, secure system administration, and risk management activities, current offerings[4] include two sets of courses. One set is built around computer security response teams and incident handling. This set includes Managing Computer Security Incident Response Teams and Computer Security Incident Handling for Technical Staff [Introductory and Advanced].

The second set is built around fundamental concepts and selected practices for Internet security. This set includes Concepts and Trends in Information Security, Information Security for System Administrators, Managing Risks to Information Assets, and The Executive Role in Information Security: Risk and Survivability. Selected, tailored training courses have also been developed to accompany security improvement modules and practices for implementation at customer organizations.

Arguably, current training for system and network administrators, their managers, and users does not sufficiently address requisite knowledge, skills, and abilities for securing networked systems unless an organization has clearly identified its critical information assets and defined a set of protection strategies that guide the appropriate training. Since the technology changes rapidly, people need to update their skills frequently. Consequently, course content needs to be dynamic as well. Thus, any systematic effort to train and certify system and network administrators must account for changing technical requirements and course content.

There is a growing demand to establish a minimum set of core competencies or certification standards for system and network administrators. Several efforts are underway to address this problem. For example, the *Information Technology Security Training Requirements: A Role- and Performance-Based Model* [7] outlines an information technology security body of knowledge, topics, and concepts. Integrated Space Command and Control[5] offers the designation of Certified Information Systems Security Professional. System Administration Networks and Security[6] offers Levels 1 and 2 certification. USENIX System Administrator's Guild[7] is currently examining certification approaches and conducting job analyses to establish standards [8].

Summary

This article described the growing problem of protecting networked systems connected to public networks such as the Internet. We presented an emerging structure for improving the security of networked systems that includes conducting an information security risk assessment, which produces a recommended set of risks to be managed and protection strategies intended to mitigate those risks. Implementing protection strategies includes adopting recommended security practices. Both assessment and practice deployment require appropriate training, which, in the future, will hopefully build upon a set of security certification standards.

We welcome your feedback and look forward to hearing about your experiences as you improve the security of your organization's networked systems and work to sustain them.◆

References

1. Allen, Julia. *Securing Networked Systems: A Technology Improvement Process.*1999 Software Engineering Process Group Conference, Carnegie Mellon University, Software Engineering Institute, March, 1999. Available at www.cert.org/sepg99/index.htm
2 Computer Security Institute, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends,* Vol. VI, No. 1, (Spring 2000).
3. Pethia, Richard. *Internet Security Issues: Testimony Before the U.S. Senate Judiciary Committee.* Carnegie Mellon University, Software Engineering Institute, May 25, 2000. Available at www.cert.org/congressional_testimony/Pethia_testimony25May00.html
4 West-Brown, Moira and Allen, Julia. SEI Interactive. Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, September 1999. Available at http://interactive.sei.cmu.edu/Columns/Security_Matters/1999/September/Security.sep99.pdf
5. Alberts, Christopher; Behrens, Sandra G.; Pethia, Richard D.; and Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE℠) Framework, Version 1.0.* (CMU/SEI-00-TR-017). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, June 1999. Available at www.sei.cmu.edu/publications/documents/99.reports/99tr017/

99tr017abstract.html
7. Wilson, William, ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (Publication 800-16). National Institute of Standards and Technology, U.S. Department of Commerce, 1998.
6. West-Brown, Moira J.; Stikvoort, Don; and Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams* (CMU/SEI-98-HB-001). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, 1998. Available at www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html
8 Laswell, Barbara; Simmel, Derek; and Behrens, Sandra G. *Information Assurance Curriculum and Certification: State of the Practice* (CMU/SEI-99-TR-021). Pittsburgh, Pa.: Carnegie Mellon University, Software Engineering Institute, July 1999. Available at www.sei.cmu.edu/publications/documents/99.reports/99tr021/99tr021abstract.html

Notes

1. Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.
2. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.
3. See www.cert.org/security-improvement
4. The current description of public offerings is available at www.sei.cmu.edu/products/courses/courses.html
   The current schedule of public offerings is available at www.sei.cmu.edu/products/calendars/calendar.html
5. See www.isc2.org
6. See www.sans.org
7. See www.usenix.org

About the Authors

Julia Allen is a senior member of the technical staff working in security improvement. She has an master's degree in electrical engineering from the University of Southern California.

Christopher Alberts is a member of the technical staff working in information security risk management. He has an master's degree in engineering from Carnegie Mellon University.

Sandi Behrens is a senior member of the technical staff working in information security risk management. She has a doctorate degree from the University of Pittsburgh with an emphasis on instructional technology and cognitive science.

Barbara Laswell is the technical manager of practices development and training. She has a doctorate degree from Stanford University in the design and evaluation of educational systems.

William Wilson is currently managing the survivable network management team. He has a master's degree in computer systems management from the University of Maryland.

Carnegie Mellon University, Software Engineering Institute
4500 Fifth Ave.
Pittsburgh, Pa. 15213
Voice: 412-268-6942
Fax: 412-268-6989
Email: Julia Allen: jha@sei.cmu.edu
Christopher Alberts: cja@sei.cmu.edu
Sandi Behrens: sgb@sei.cmu.edu
Barbara Laswell: blaswell@sei.cmu.edu
William Wilson: wrw@sei.cmu.edu
Internet: http://www.sei.cmu.edu, http://www.cert.org

Quote Marks

Those who can, compute.
Those who cannot, program.
Those who can't program, write manuals.
Those who can't write manuals, sell computers. *- Anon.*

A computer lets you make more mistakes faster than any invention in human history, with the possible exception of handguns and tequila.

Mitch Ratcliffe, "Technology Review" (1992)

Computer accomplishments will be of ultimately greater significance to civilization than those of space technology or nuclear physics. *Walter F. Bauer*

The Survivability Imperative: Protecting Critical Systems

By Richard C. Linger, Robert J. Ellison, Thomas A. Longstaff, and Nancy R. Mead
Software Engineering Institute

The success of virtually all organizations in defense, government, and business is dependent on availability and correct functionality of large-scale networked information systems of remarkable complexity. Because of the severe consequences of failure, organizations are focusing on system survivability as a key risk management strategy. The Survivable Network Analysis (SNA) method provides a systematic means to assess and improve system survivability for risk reduction. Survivability can also be integrated into requirements definition for new or evolving systems.

Progress Demands System Survivability

Modern society is increasingly dependent upon large-scale, highly distributed systems that operate in unbounded network environments. Such systems improve efficiency by permitting entire new levels of organizational integration, but they also introduce elevated risks of intrusion and compromise. These risks can be mitigated within the organization's system by incorporating survivability capabilities.

Unbounded networks such as the Internet have no central administrative control and no unified security policy. Furthermore, the number and nature of nodes connected to such networks cannot be fully known. Despite the best efforts of security practitioners, no amount of hardening can assure that a system connected to an unbounded network will be invulnerable to attack.

The discipline of survivability can help ensure that systems can deliver essential services and maintain essential properties including integrity, confidentiality, and performance despite the presence of intrusions. Unlike traditional security measures, which often depend on central control and administration, survivability is intended to address network environments where such capabilities may not exist.

Survivability is defined as the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks, failures, or accidents. As an emerging discipline, survivability builds on related fields of study, including security, fault tolerance, safety, reliability, reuse, performance, verification, and testing; moreover, it introduces new concepts and principles [1, 2, 3, 4, 5]. Survivability focuses on preserving essential services in unbounded environments, even when systems are penetrated and compromised.

In defining survivability, the term mission refers to high-level organizational objectives. Missions are not limited to military settings; any successful organization or project must have a vision of its objectives, whether expressed implicitly or as a formal mission statement. Judging mission fulfillment is typically made in the context of external conditions that affect achievement of mission objectives.

For example, a financial system may shut down for 12 hours during a period of widespread power outages caused by a hurricane. If the system preserves integrity and confidentiality of data and resumes essential services following the period of downtime, it can reasonably be judged to have fulfilled its mission. However, if the system shuts down unexpectedly for 12 hours under normal conditions or minor environmental stress and deprives users of essential financial services, it can be judged to have failed its mission, even if integrity and confidentiality are preserved.

Glossary of Survivability Terms

Accidents—A broad range of randomly occurring and potentially damaging events such as natural disasters. Accidents are often externally generated events.

Adaptation services—Survivable system functions provided to continually improve a system's capability to deliver essential services, typically by improving resistance, recognition, and recovery capabilities.

Attack—A series of steps taken by an intelligent adversary to achieve an unauthorized result. Attacks include intrusions, probes, and denials of service.

Essential services—Services that must be provided to system users even in the presence of attacks, failures, or accidents.

Failure—A potentially damaging event that results from deficiencies in a system or in an external element on which the system depends. Failures may be due to results from software design errors, hardware degradation, human errors, or corrupted data.

Recognition services—Survivable system functions that must detect attempted and successful attacks.

Recovery services—System functions to support the restoration of services after an attack. Recovery services also contribute to a system's ability to maintain essential services during an attack.

Resistance services—System functions that repel attacks and make them difficult and costly.

Survivability—A system's capability to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

Unbounded network—A computer system or systems characterized by distributed administrative control without central authority, limited visibility beyond the boundaries of local administration, and lack of complete information about the network.

Timeliness is typically a critical factor in mission objectives, and is explicitly included in the definition of survivability. The terms attack, failure, and accident include all potentially damaging events; however, these terms do not partition events into mutually exclusive or even distinguishable sets. It is often difficult to determine if a particular detrimental event is the result of a malicious attack, a component failure, or an accident. Even if the cause is eventually determined, the critical immediate response cannot depend on speculations about the cause.

Attacks are potentially damaging events orchestrated by an intelligent adversary. Attacks include intrusions, probes, and denials of service. Moreover, the threat of an attack can have as severe an impact on a system as an actual occurrence. A system that assumes an overly defensive position because of an attack threat may significantly reduce functionality and divert excessive resources to monitoring the environment and protecting system assets.

Failures are potentially damaging events caused by deficiencies in a system or in an external element upon which the system depends. Failures may be due to software design errors, hardware degradation, human errors, or corrupted data.

Accidents describe a broad range of randomly occurring and potentially damaging events, such as natural disasters, that usually originate outside a system.

With respect to survivability, a distinction between an attack and failure or accident is less important than the impact of the event. It is often not possible to distinguish between intelligently orchestrated attacks and unintentional or random detrimental events. Survivability concentrates on the effect of a potentially damaging event. For a system to survive, it must recover from a damaging effect long before the underlying cause is identified. In fact, recovery must be successful whether or not the cause is ever determined.

It is important to recognize that mission fulfillment must survive—not any particular subsystem or component. The core concept of survivability is the capability of a system to fulfill its mission, even if significant portions of the system are damaged or destroyed.

Survivable Network Analysis

The SNA method depicted in Figure 1 was developed by the SEI Computer Emergency Response Team (CERT) Coordination Center as a practical engineering process for systematic assessment of survivability properties of proposed systems, existing systems, and modifications to existing systems [6, 7]. SNA is carried out at the architecture level as a cooperative project by an SEI team working with system architects, developers, and stakeholders. The method proceeds through a series of joint working sessions, culminating in a briefing on findings and recommendations. In this article, the focus is on attacks, although the trace-based, compositional SNA method applies to analysis of failures and accidents as well.

The SNA method provides a means for organizations to understand survivability in the context of their operating environments. What functions must survive? What intrusions could occur? How could intrusions affect survivability? What are the risks to the mission? How could architecture modifications reduce the risks? Systematic consideration of these questions through SNA reveals the risks and leads to mitigation strategies. Steps in the SNA method are defined as follows:

Step One: System Definition

The first step focuses on understanding mission objectives, requirements for the current or candidate system, structure and properties of the system architecture, and risks in the operational environment.

Step Two: Essential Capability Definition

Once step one is complete, essential services (services that must be maintained during attack) and essential assets (assets whose integrity, confidentiality, availability, and other properties must be maintained during attack) are identified, based on mission objectives and the consequences of failure. Essential service and asset uses are characterized by usage scenarios, which are traced through the architecture to identify essential components whose survivability must be ensured.

Step Three: Compromisable Capability Definition

Next, intrusion scenarios are selected based on assessment of environmental risks and intruder capabilities. These scenarios are likewise mapped onto the architecture as execution traces to identify corresponding compromisable components (components that could be penetrated and damaged by intrusion). In essence, intruders are treated as simply another class of users, and the design task for intrusion usage is to make it as difficult and costly as possible.

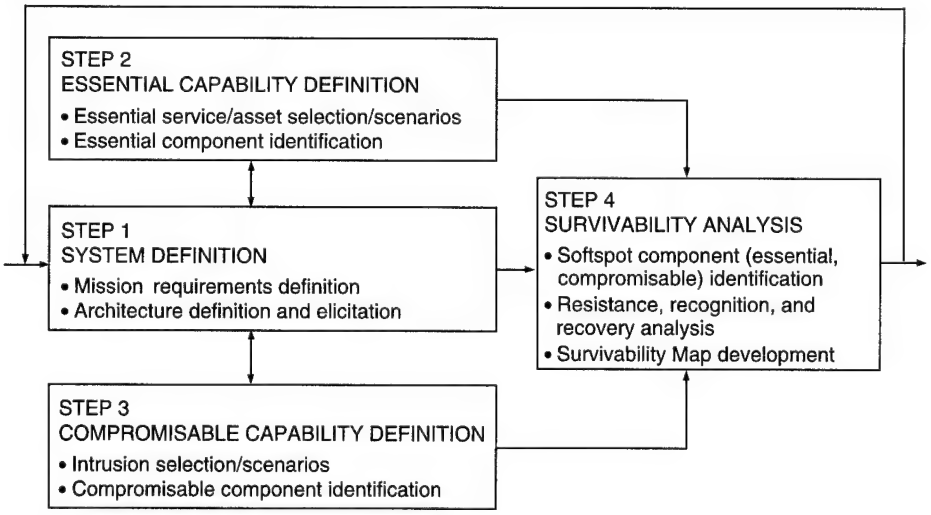
Step Four: Survivability Analysis

The final step of the SNA method takes aim at soft spot components of the architecture. These are components that prove both essential and compromisable, based on the results of steps two and three. Soft spot components and supporting architecture are then analyzed for the key survivability properties of resistance, recognition, and recovery (the three Rs), as well as for adaptation and evolution.

Resistance is the capability of a system to repel attacks. Recognition is the system's capability to detect attacks as they occur and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability, is the capability to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack. Table 1 depicts some strategies for improving survivability.

The analysis of the "three R's" is summarized in a Survivability Map as depicted in Figure 2. The map enumerates, for every intrusion scenario and its corresponding soft spot effects, the current and recommended architecture strategies for resistance, recognition, and recovery. The Survivability Map provides feedback about the original architecture and system requirements, and gives management a roadmap for survivability evaluation and improvement. In addition, survivability analysis often results in recommendations for security and survivability policy definition or modification. The SNA method has been applied to a number of systems with good results.

Figure 1. *The Survivable Network Analysis Method*



Key Property	Description	Examples
Resistance to attacks.	Strategies for repelling attacks.	System and user authentication, access control, encryption, fire walls, proxy servers, strong configuration management, dispersion of data, diversification of programs, application of system upgrades for known vulnerabilities.
Recognition of attacks and extent of damage.	Strategies for detecting attacks (including intrusions) and understanding the current state of the system, including evaluating the extent of the damage.	Recognition of intrusion usage patterns, virus scans, internal integrity checking, auditing, system configuration and network monitoring.
Recovery of full and essential services after attack.	Strategies for restoring compromised information or functionality limiting the extent of damage, maintaining or, if necessary, restoring essential services within the time constraints of the mission, restoring full service as conditions permit.	Restoration of data and programs, use of alternative services, operational procedures to restore system configurations, isolation of damage, ability to operate with reduced services or reduced user community.
Adaptation and *evolution* to reduce effectiveness of future attacks.	Strategies for improving system survivability based on knowledge gained from intrusions.	Incorporation of new patterns for intrusion recognition, adaptive filtering and logging.

Table 1. *Some Strategies for Improving System Survivability*

Customers have benefited from survivability improvements to system architectures, as well as from clarified requirements and early problem identification. Survivability is also the subject of ongoing research, as described, for example, in Fisher [8].

Adding Survivability to System Requirements

Survivability properties can also be integrated into the requirements definition for new or evolving systems [9]. Figure 3 depicts an iterative model for defining survivable system requirements. Survivability must address not only requirements for software functionality, but also requirements for software usage, development, operation, and evolution. Thus, five specific types of requirements definitions are relevant to survivable systems in the model of Figure 3, as discussed below.

System/Survivability Requirements

In this discussion, system requirements refers to traditional user functions that a system must provide. For example, a network management system must provide user functions for monitoring network operations, adjusting performance parameters, and so forth. System requirements also include non-functional aspects, such as timing, performance, and reliability. Survivability requirements refer to system capabilities for the delivery of essential services in the presence of attacks and intrusions, and recovery of full services.

Survivability requires that system requirements be organized into essential services and non-essential services, perhaps in terms of user categories or business criticality. Essential services must be maintained even during successful intrusions; non-essential services are to be recovered after intrusions have been dealt with.

Essential services may be further stratified into levels with each embodying fewer and more vital services as a function of increasing severity and duration of intrusion. It is also possible that the set of essential services may vary in a more dynamic manner depending on a particular attack scenario and the resulting situation. In this case, services that are essential under one scenario may not be essential under another resulting in different combinations of essential services that are scenario-dependent.

Thus, definitions of requirements for essential services must be augmented with appropriate survivability requirements. As shown in Figure 3, survivable systems may also include legacy and COTS components not originally developed with survivability as an explicit objective. Such components may provide both essential and non-essential services and may engender special functional requirements for isolation and control through wrappers and filters to help permit safe use in a survivable system environment.

Beyond functional requirements, survivability itself imposes new types of requirements on systems for resistance to, recognition of, and in particular, recovery from intrusions and compromises. A variety of existing and emerging survivability strategies, noted in Table 1 support these survivability requirements.

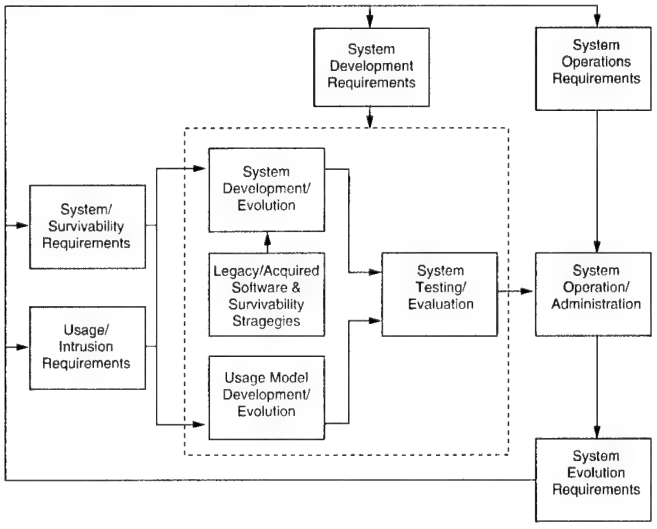
Survivable systems are envisioned as capable of adapting their behavior, function, and resource allocation in response to intrusions. When necessary, for example, functions and resources devoted to non-essential services could be reallocated to the delivery of essential services and intrusion resistance, recognition, and recovery. Requirements for such systems must specify the behavior for adaptation and reconfiguration in response to intrusions.

Systems can exhibit large variations in survivability require-

Figure 2. *Sample Survivability Map Format*

Intrusion Scenario	Softspot Effects	Architecture Strategies for:	Resistance	Recognition	Recovery
(Scenario 1)		Current			
...		Recommended			
(Scenario n)		Current			
		Recommended			

Figure 3. *Requirements Definition for Survivable Systems*



ments. Small local networks may have few or even no essential services with acceptable manual recovery times measured in hours. Large-scale networks of networks may be required to maintain a core set of essential services with automated intrusion detection and recovery times measured in minutes. Embedded command and control systems may require essential services to be maintained in real time, with recovery periods measured in milliseconds. Attainment and maintenance of survivability consumes resources in system development, operation, and evolution. Survivability requirements for a system should be based on costs and risks to an organization associated with loss of essential services.

Usage/Intrusion Requirements

Survivable system testing must demonstrate the performance of essential and nonessential system services, as well as the survivability of essential services during an intrusion. Because system performance in testing (and operation) depends totally on the usage to which it is subjected, an effective approach to survivable system testing is based on usage scenarios derived from usage models.

Usage models are developed from usage requirements, which specify legitimate usage environments and all possible usage scenarios. Usage requirements for essential and nonessential services must be defined in parallel with system and survivability requirements. Furthermore, intrusion usage must be treated on a par with legitimate usage and intrusion requirements, which specify that intrusion usage environments and all possible scenarios of intrusion use must be defined as well. In this approach intrusion usage is modeled in conjunction with the legitimate use of system services. Intruders may engage in usage scenarios beyond legitimate scenarios, but may also employ legitimate usage for purposes of intrusion if they become privileged to do so.

Development Requirements

Survivability places stringent requirements on system development and testing practices. Software errors can have a devastating effect on survivability and provide ready opportunities for intruder exploitation. Sound engineering practices are required to create survivable software. The following five principles—four technical and one organizational—are example requirements for survivable system development and testing practices:

- Precisely specify required functions in all possible circumstances of use.
- Verify correct implementations with respect to function specifications.
- Specify function usage in all possible circumstances of use, including intruder usage.
- Test and certify based on function usage and statistical methods.
- Establish permanent readiness teams for system monitoring, adaptation, and evolution.

Sound engineering practices are required to deal with legacy and COTS software components as well.

Operations Requirements

Survivability also places demands on requirements for system operation and administration to define and administer survivability policies, monitor system usage, respond to intrusions, and evolve system functions as necessary to ensure survivability as usage environments and intrusion patterns change over time.

Evolution Requirements

Lastly, system evolution is an inevitable necessity in response to users' requirements for new functions and intruders' increasing knowledge of system behavior and structure. In particular, survivability requires that system capabilities evolve more rapidly than intruder knowledge. This prevents the accumulation of information about invariant system behavior and structure needed for an intruder to achieve successful penetration and exploitation.

Summary

The emerging discipline of survivable systems is directed at maintaining essential mission operations in adverse circumstances that no amount of security precautions can guarantee to prevent. System survivability can be investigated and improved through the SNA method, and survivability can be integrated into system requirements on a par with functionality and performance. Survivability analysis is a prudent risk management technique in a world of increasing dependency on complex, large-scale network systems.◆

References

1. Lipson, H.F. and Fisher, D.A. *Survivability—A New Technical and Business Perspective on Security,* Proceedings of the New Security Paradigms Workshop, IEEE Computer Society Press, 1999.
2. Presidential Commission on Critical Infrastructure Protection, *Critical Foundations—Protecting America's Infrastructures,* The Report of the Presidential Commission on Critical Infrastructure Protection, October 1997, p. 173., Available at www.pccip.gov
3. DARPA Information Survivability Program. Available at www.darpa.mil/ito/research/is
4. Proceedings of the 1997 Information Survivability Workshop, San Diego, Calif., Feb. 12–13, 1997, SEI and IEEE Computer Society, April 1997. Available at www.cert.org/research
5. Proceedings of the 1998 Information Survivability Workshop, Orlando, Fla., Oct. 28–30, 1998, SEI and IEEE Computer Society, 1998. Available at www.cert.org/research
6. Ellison, R.J., Linger, R.C., Longstaff, T., and Mead, N.R. Survivable Network Systems Analysis: A Case Study, *IEEE Software,* July/August 1999, pp. 70-77.
7. Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A., and Mead, N.R. Survivability: Protecting Your Critical Systems, *IEEE Internet Computing,* November/ December 1999.
8. Fisher, D.A. and Lipson, H.F. *Emergent Algorithms—A New Method for Enhancing Survivability in Unbounded Systems,* Proceedings of the 32nd Annual Hawaii International Conference on System Sciences, Maui, Hawaii, Jan. 5—8, 1999 (HICSS-32), IEEE Computer Society, 1999.
9. Linger, R.C., Mead, N.R, and Lipson, H.F. *Requirements Definition for Survivable Network Systems,* Proceedings of International Conference on Requirements Engineering, IEEE Computer Society Press, Los Alamitos, Calif.,1998, pp. 14-23.

Continued on page 25 ☞

Avoiding the Trial-By-Fire Approach to Security Incidents

By Moira West-Brown
Computer Emergency Response Team (CERT®) Coordination Center, Software Engineering Institute

Being proactive about security is critical to mitigating your security risk. However, having good security measures in place will not prevent you from suffering computer security incidents. So it is also important to be prepared and proactive about detecting and responding to such incidents when they do arise. This article explores the range of options that exist in organizations today for detecting and responding to security incidents.

Some Just Get Burned

Experience shows that most organizations do not think about how to respond to a computer security incident until after they have been hit significantly. They have not assessed the business risk of not having formal incident-detection and response mechanisms in place. More often than not, organizations receive reports informing them that they are involved in an incident originating from some other party rather than identifying the incident themselves. This is called the trial-by-fire approach.

The problem stems from a lack of organizations recognizing their need for a comprehensive security infrastructure. It is not until after an ill-prepared organization has suffered a significant security incident that business risk and impact are realized. The management may perceive that network and host security is something that the system and network administrators handle as a part of their day-to-day activities. Or they may think that security is handled by the organization's firewall.

Sadly this perception is often incorrect on both counts. The staff priorities are primarily focused on maintaining basic support and operation of the vast amount of computing equipment in place. Firewalls may prevent some attacks, but cannot prevent all attack types; and, if not correctly configured and monitored, they may still leave the organization open to a range of others. This approach, or lack of one, results in significant problems such as:

- Not knowing if or for how long a network or systems have been compromised.
- Not knowing what information is at risk, has been taken, or has been modified by intruders.
- Not understanding methods perpetrator(s) use to gain access to systems.
- Not understanding what steps can be taken to stop the intrusion activity and secure the systems and network.
- Not identifying in advance any possible adverse effects incident response actions may have on the company's ability to conduct business.
- Not knowing who has authority to make decisions related to containing the activity, contacting the legal department, law enforcement, etc.
- Delays in identifying and contacting the right people to notify about the activity (internally and externally).
- No recognized reporting contact in the organization known to external or internal parties.

The Volunteer Approach

Some organizations have system and network administrators who are either interested or trained in computer security. Such individuals are better prepared to address security within their domain of authority—such as the machines in one department or operating unit, or the equipment on a given network segment.

Within some organizations, various individuals may be working together to address security needs informally. This approach often stems from a group of individuals in the organization who see the need to address security even if the need is not recognized by higher level management.

However, even having capable people available does not mean that the organization is prepared to respond. Depending on the scope of the overall volunteer effort, it is likely that even with intrusion-detection software in place in parts of the organization, serious network security incidents may still go undetected. Although this approach is a marked improvement over the trial-by-fire approach, significant problems still remain, including:

- Serious intrusions may still go undetected.
- Volunteers may be able to deal with the technical issues, but may not understand or have the information available to assess the business consequences of any steps taken.
- Volunteers may not have the authority to apply the technical steps (e.g., disconnecting the organization from the Internet) or other actions they believe are necessary (e.g., reporting the activity to law enforcement or seeking the advice of legal counsel).
- Volunteers may delay seeking and obtaining management approval to respond.
- Volunteers have no bigger picture of the overall detection and response activity.
- Volunteers may know in some cases whom to contact internally, but anomalies may exist.
- Other individuals in the company who identify a possible security incident may not be aware of the informal group and may fail to report to it.
- An informal group is unlikely to have external recognition and support.

The Company-Supported Approach

Despite good intentions of technical experts or other staff members, the only effective approach to incident detection and response is to make it part of an organization-wide risk-management plan founded on the highest level of management support. Regardless of how such an approach is implemented—whether by a geographically distributed or centrally located team consisting of full- or part-time staff, or supplemented with contract support—without management support the effort will struggle to succeed. In addition to the foundation of management support, the empowered group must also be recognized internally and externally and prove its effectiveness, trustworthiness, and ability to everyone.

Management authority and recognition are the foundation for success. But

an effective detection and response service needs the trust and respect of the constituency served and others with whom the service will need to interact.

Teams established to address incident detection and response for organizations are known as computer security incident response teams (CSIRTs). Forming, staffing, and operating a CSIRT is not easy. However, if appropriately set up and empowered within an organization, a CSIRT can begin to gain the trust and respect necessary to address incident detection and response from a company-wide perspective.

CSIRTs vary in structure, staffing, and the range of services provided based on the situation or need that they are trying to fulfill. Consider the need for a CSIRT in your own organization, whether it is company wide or just for your business unit or department. A recently published handbook is available at www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html to help an organization determine the scope and range of services for a CSIRT and provide guidance in forming operational policies and procedures.

Advocating the Company-Supported Approach

Making the transition from a trial-by-fire or volunteer response effort to a company-supported one is not easy. The most important and often the most difficult challenge is convincing management of their need for an effective and empowered CSIRT as part of an overall risk-management approach.

Waiting for a serious security incident to occur within your organization to convince management of the need is not a productive approach. Nor will it necessarily be successful. Even after suffering a serious computer-security incident comprimising hundreds of systems, some organizations still do not recognize the need for a formal incident-response capability.

I remember one case in which I contacted a multinational company to provide information indicating that an intruder was gaining access to the company's corporate network through the Internet. As a result of the report, the company began to look at its systems and found that they had been seriously compromised for more than six months. The company was able to identify many systems and internal networks that were compromised by the activity along with the sensitive information available on those systems. But it had no idea of the intruder's motives or the extent of the data that the intruder had copied or amended. A significant period of time elapsed and further compromises occurred before the organization established a CSIRT.

> "It is only a matter of time before insurance companies begin to request more information about network security and to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer security incidents."

Another organization that was compromised by an intrusion reinstalled all of its systems from known good backups—losing two weeks of production effort in the process—as they could not be certain what data might have been tampered with by the intruder. In this case, malicious modifications to the application under development could have resulted in loss of life if the application had failed during use. The organization involved promptly established a company-supported CSIRT.

One of the most important factors to document is the associated business risk or loss of any incident. This information must be presented in a form that will help management understand that the problem is a business one and not a technical one. I recall one case in which technical staff had great difficulty in gaining management attention regarding ongoing intrusions. It was not until the intrusion data was presented by describing the mission of each system in question rather than providing its host name and operating system version that management paid attention. Volunteers should attempt to document and present to management the impact of known intrusions and recorded losses.

The Insurance Influence

I learned of one situation recently in which a security officer compromised the home system of a manager as a last resort to gain management recognition of the company's security risk. For the majority of us, such extreme measures are far too dangerous. In such cases, financial pressure from another source may be a last resort to gain management's attention. Pressure from insurance companies (seeking to limit exposure of losses resulting from network security incidents) will provide a financial incentive for organizations to improve security measures to keep insurance premiums affordable.

I was involved in a recent insurance application where an insurance company requested information on what policies an organization had in place for virus prevention and control of defamatory or libelous information on public Web sites and mailing lists. Conspicuous by their absence were questions seeking an understanding of how well prepared the organization was to prevent, detect, and respond to computer security incidents—even if only from the perspective of preventing viruses or defamatory or libelous information being published on a public forum.

It will not be long before insurance companies are asking the right questions in this area. In fact some already are, but their motives are slightly different. Just recently some insurance companies have begun to offer policies that provide organizations with financial protection for third-party damages resulting from network security breaches. A prerequisite for such coverage is an associated network security risk assessment.

It is only a matter of time before insurance companies begin to request more information about network security and to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer security incidents. Eventually, trial-by-fire or financial incentives will force organizations to realize the need for a CSIRT.

Be Prepared

It is still not uncommon to find callers to the CERT Coordination Center hotline who do not know what steps to take to report an incident within their own organizations. Although many callers know their vendor and maybe even the organization's Internet service provider,

very few know to whom they should report a computer security incident. Being prepared and knowing what to do in advance can help to further mitigate the damage. That is why it is very important that an organization advertise its CSIRT both internally and externally. As with emergency services, it is important to find out how to contact a CSIRT before it is needed in an emergency. It is also important to know in advance whom the service can help and what information is needed to ensure that the CSIRT can provide the service requested.

To find out if your organization has a company-supported CSIRT, ask your security officer or system/network administrator, and consult your organization's security policies and practices. Some CSIRTs are members of the Forum of Incident Response and Security Teams (FIRST). See www.first.org/ team-info for a list of FIRST members and their contact information

With millions of organizations now reliant on networks to conduct their businesses, it is a shocking fact that only a few hundred CSIRTs exist around the world today. Many of these CSIRTs continue to cite annual increases of 200 percent or 300 percent in the numbers of computer security incidents reported to them. They are struggling to keep pace with the number of incoming reports. Even with general improvements in the field of network security, a dramatic increase in the number of CSIRTs is urgently needed. More advocates are needed to help organizations understand the risks associated with the failure to detect and appropriately respond to computer security incidents.◆

About the Author

Moira J. West-Brown is a senior member of the technical staff within the CERT® Coordination Center at the Software Engineering Institute. She leads a group that aids in forming new CSIRTs world wide. Active in CSIRT internationally, she has developed a variety of materials on operational and collaborative CSIRT issues. She was elected to the Forum of Incident Response and Security Teams Steering Committee in 1995 and is currently chair. She holds a bachelor's degree in computational science from the University of Hull, United Kingdom.

Open Forum

Security Often Sacrificed for Convenience

By Shawn Hernan
Vulnerability Handling Group, CERT® Coordination Center

When given a choice between a product that is secure and one that is not, nearly everyone will say they would prefer the secure product, all else being equal. But things are not equal. Despite clients' cries for more secure products from vendors, when it comes to writing the check security often gets the short end of the stick.

The Message Clients Send

One e-mail product vendor has been among the market leaders in implementing security features into its products. This vendor, who ships both e-mail servers and e-mail clients, was among the first to add a particular kind of secure authentication to client and server. As the vendor was among the first to do so, there were concerns about interoperability. Would its e-mail client be able to work with other vendors' e-mail servers, and vice-versa? Would the secure authentication scheme prevent interoperation with other vendors' products?

Complicating matters was the fact that the e-mail protocol did not provide for explicit failure messages when an authentication attempt failed. That is, the client was unable to tell if the authentication attempt failed because the password was incorrect, or because the server did not support the same authentication scheme. Here were possible options if the client received a failure message:

- Ask the user for the password again, assuming it was incorrect the first time.
- Try a less secure but more widely implemented authentication scheme, namely plain text passwords.

In other words, the vendor was faced with a tradeoff between interoperability and security by default. The vendor chose security by default and started to ship the client. The default behavior was to stick with the secure authentication scheme, but give the end user a way to configure it so the client could use a less secure authentication scheme.

The effect of this security-conscious choice was that the client would work only with a server from the same vendor, until other vendors implemented the same authentication scheme. The vendor provided documentation with the product to allow an end user to configure the product to work with other vendors' servers. So the issues of security and interoperability were addressed, but security was primary.

Although the end user could configure the product to work with other vendor's servers, the vendor received more than 280 trouble reports from sites that thought the client was broken or that simply did not want to reconfigure the client. The customers wanted interoperability by default.

This market pressure forced the vendor to choose a different set of defaults—the product will now try less secure authentication schemes if the more secure scheme fails. Thus, if a user makes an error in typing a password, the client will try the same incorrect password using all of the authentication schemes including plain text.

This means that if the user makes a typo in entering a password, the slightly incorrect password is sent on the network in plain text. More importantly, if an intruder is able to convince a user to establish a connection to a mail server of the intruder's choice, the intruder can recover the user's password. The consequence of the customers' demands for default interoperability was that they obtained a less secure product.

Having changed the default configuration of the product, we would expect that the vendor would have received trouble reports from other customers complaining about the less secure configuration. But they received only one such report. The message sent to this vendor was loud and clear—default interoperability is more important than default security.

Standardization

Many organizations are under pressure to standardize on one set of applications, operating systems, servers, firewalls, and routers. Standardization can reduce your costs, but also reduces your resistance to catastrophic outages during widespread security events like the Melissa macro virus or the Love Letter visual basic script.

Biological analogies are useful here. Genetic diversity increases the ability of the population to survive in the face of a virulent parasite or disease. Likewise with technology, if your entire organization is comprised of a single platform then your risk of catastrophic loss is higher.

Despite the risks, many organizations are standardizing on small sets of platforms and applications in an effort to save money (sometimes without actually evaluating the total costs of ownership) without accounting for the risks of catastrophic failure.

Again, the message to vendors and system integrators is clear: *sameness* is more important than security.

The User Experience and Mobile Code

Many Web sites use ActiveX, JavaScript, Java, or dynamic HTML to enhance their pages often strictly for aesthetic reasons. But this use of mobile code has sometimes become part of the functionality of the site. Many electronic commerce sites, for example, require the use of JavaScript or ActiveX to complete the transaction. This has led to a serious quandary: Whenever a problem is discovered in any of the mobile code technologies, it is not practical to disable that technology.

Many Web sites, for example, are still vulnerable to the "Cross-site Scripting" attack described in CERT Advisory CA-2000-02, yet have not removed the offending code from their Web sites. Thus, users of that site may be vulnerable if they have decided to trust it. The nature of the vulnerability is that malicious code can be injected from a trusted site into your browser.

Sites are competing on functionality and appearance, and that's how they're being evaluated. In my experience, clients are unwilling to forgo mobile code technology, despite the risks it presents, even when alternatives are available. Again, the message is loud and clear—security is less important than functionality or even appearance.

Conclusion

Security is not only for security products like firewalls and encryption software. The great majority of the problems we see are a result of flaws in ordinary programs. Things like mail servers, spreadsheets, word processors, help programs, Web servers, and all the things we use everyday are the same things that intruders use to gain unauthorized access to your systems.

Security products certainly help, but they are not a substitute for secure programs and protocols. Unless you behave like security really matters—and it does—then you will not get it. And you will not be secure.◆

About the Author

Shawn Hernan is a member of the technical staff at the CERT® Coordination Center where he leads the Vulnerability Handling Group. Prior to joining CERT®/CC, Shawn worked for the Systems and Networks division of the University of Pittsburgh for seven years where he developed databases and network applications, and shared in the system administration of the centralized computing facilities and the large campus network.

Network Security Web Sites

www.disa.mil/line/disalin5.html
This is the site by the Defense Information Systems Agency for Center for Information System Security.

www.vtcif.telstra.com.au/info/security.html
The Computer and Network Security Reference Index's links include frequently asked questions on topics such as Internet firewalls, computer security, and Web security; online document archive relating to network and computer security; and newsgroups.

www.alw.nih.gov/Security
This page features general information about computer security. Its links include advisories of groups around the world on security vulnerabilities and methods to remove or reduce those dangers; articles on computer and network security; and electronic magazines, newsletters, and news sites devoted to this topic.

http://computingcentral.msn.com/topics/safecomputing
This site includes a Safe Computing Forum and talks about how to use firewalls as a protection from computer viruses and hackers.

www.andrew.cmu.edu/~zu22/html/security/security.html
This is a 21-page listing of network security resources.

www.fish.com/satan
See this site for information about the Security Administrator's Tool for Analyzing Networks.

http://netsecurity.about.com/compute/netsecurityi/msub25.htm?rnk=r1&terms=kevin+mitnick
Devoted to articles on computer hacker Kevin Mitnick, including a long article he wrote from the federal detention center.

www.alw.nih.gov/Security/security-docs.html
This site contains miscellaneous documents about various computer security issues that are loosely organized by subject area.

www.gocsi.com
Computer Security Institute's site, with links to articles on topics such as "10 Risks of PKI: Bruce Schneir Debunks the Hype."

www.p-and-e.com/pubs_nstissc.htm
Various security publications listed by the National Security Telecommunications and Information Systems Security Committee.

www.mountainwave.com
This is the site for *Computer Security News Daily.* The lengthy article links include government and business news, the Internet, hackers, products, and the law.

www.dtic.mil/dodsi/bulletin.html
Access this site for publications by the *Security Awareness Bulletin,* a publicationof the Department of Defense Security Institute. The most recent editions, however, are September and December 1997.

Electronic Commerce and Governance: A Darwinian Discussion

By Nancy Lee Hutchin
Keane Federal Systems Inc.

Technologies, processes, and interactions between government bodies and their citizens can benefit from the improvements driving the private sector economy by streamlining processes to improve the quality of consumer/customer service; reducing waste, fraud, and overhead costs; and making better use of public budgets. Public-sector organizations can profit from lessons learned in the private sector where competition has fueled e-commerce expansion. This article addresses the benefits and challenges of electronic governance and e-commerce in the public sector, points to issues such as information security, and concludes with a discussion of the implications of changing the fundamental relationship between citizens and their governmental bodies.

An e-commerce strategy is *not* merely the online automation of the consumer relationship. It is the deep, fundamental redefinition of that relationship, combining a Pandora's box of security issues with a remarkable degree of autonomy and service for the consumer. However, what might begin with an offhand approach to Web-based services or the selling process can degenerate into a terrifying inability to respond to demanding customers. Retailers involved in legal battles due to last year's severely disappointed holiday shoppers know all too well how inadequate their planning or their understanding was. Perhaps in no other environment, except for life-support applications, does this quality of software demand such intense scrutiny, maintenance, and care.

Recently attorneys launched a class-action lawsuit against the online incarnation of a national toy store chain, saying the company's Web store accepted orders for toys during the 1999 Christmas rush even though it knew it would not be able to deliver purchases on time. Nine out of 10 customers who shopped the World Wide Web during the holiday season experienced problems, and 88 percent abandoned their shopping cart at some point during the visit [1]. In spite of this, U. S. consumers still spend about $29 billion annually on Web commerce, and researchers at the Wharton School of Business estimate that this figure will reach $133 billion by January 2004 [2].

Clearly a fundamental change is under way in the private sector's business practices and Internet use. But what does this have to do with the way government relates to its citizens? At the core of these relationships lies a transaction—an exchange of goods, services, or information that can be improved in the same ways as private-sector relationships. These transactions can:

- Provide better quality to the consumer/citizen.
- Improve the use of revenue/budgets.
- Reduce nonvalue-added expenditures or overhead costs.

Private/Public Sector Comparison

To be able to apply best practices from the private sector, it has to be acknowledged that there are some real differences between the world of government and commercial enterprise:

- **Government budgets.** These are invariably constrained. Unlike business, information technology (IT) success does not necessarily lead to an influx of new capital and increased budgets.
- **Politics.** All enterprises have internal politics, but the commercial world is not exposed to the frequent disruptions of changing administrations, rotating military leaders, and objectives.
- **Personnel.** Recruiting and retaining skilled IT staff is challenging for the most attractive technology firms. Government agencies are constrained by budgets, inability to offer incentives such as stock options, and less state-of-the-art work environments
- **Competition.** While most government organizations do not face the same direct competition as business, an increasing number are moving to a fee-for-service mode of operation.

Although the government originally developed the Internet, the free market recognized its opportunity and exploited the new ecology first, fueling its growth and penetration into households around the world. Entrepreneurs seeking profits developed the practical applications and businesses that propelled the Internet into an economic force. That has made Silicon Valley the gathering place and breeding ground of "dot-com" millionaires.

Competition forces fierce survival tactics. The rapid changes imposed by the online revolution quickly eliminated those businesses that could not adapt. Similarly, only the best and most practical applications and processes survive the intense competition of the commercial world. Here are some examples:

- Amazon.com entered and redefined the world of book sales and now has 10 times the market value of Barnes & Noble.
- Electronic trading redefines the world of stock trading. Merrill Lynch is forced to enter into electronic trading. What does it do with its stockbrokers? The fee structure has been totally changed (i.e., reduced) and has led to a new market segment—day traders.
- E-Bay, by offering online auctioning, has created a subindustry of traders in all sorts of commodities, especially antiques.
- Eastman Kodak is changing from a chemical company into a data manipulator as digital technology revamps photography. Polaroid is still struggling to make its transition. Why do you need an instant camera when a digital photograph is instant?

While the intense competition forces the commercial world to constantly innovate, only those innovations that prove viable and competitive will survive to maturity. As a result, the commercial world is a great source of battle-tested ideas, applications, and best practices—the same kind of revolutionary breakthroughs so needed in government.

A Model for Implementation

Adapting business and government to the Internet entails more than just creating a Web site and trying to draw as many visitors as possible. For the provision of electronic government

Figure 1. *Commercial E-Business Model.*

services to constituents, the site is only the beginning. E-business, electronic governance, and e-commerce are synonymous. This view dramatically understates the value, potential service, and efficiency gains offered by integrating all aspects of an enterprise.

To achieve its full potential, the new electronic world interconnects front-office and back-office operations, integrating rather than replacing legacy applications. As alluded to earlier, it goes beyond simple technological implementation to a comprehensive rethinking of the processes, organizational structures, technology architectures, and all their interfaces. Figure 1 shows the potential for integration in the commercial world.

While recognizing the many differences between government and commercial organizations, this business model can be adapted to fit the needs of a government entity. Some of the differences are simply terminology while other cases will require an adaptation of business-oriented functions to serve a different, but related, government need. Figure 2 lays out this approach.

In this model, the customers from the business model become the constituents of government—its citizens and businesses. Back office operations are almost identical to those in a business. The government procures goods and services, sends and receives bills, delivers services, and must manage its finances and risks. Business-to-business services, such as online trading communities, have provided the auto manufacturers and other industry segments with tremendous savings in their procurement processes. Applying these concepts, and rethinking procurement regulations to enable efficient online trading, could provide governments with significant cost savings and competitive advantages.

Enterprise management functions in electronic government are also quite similar, although the emphasis may be different. All organizations are faced with recruiting, training, and supporting employees. Constituent relations in the business world refer to

Figure 2. *Electronic Government Model*

systems supporting investors, analysts, and the press. In the public sector, the investors are the taxpayers. In both cases, the investors want to know that their money is well spent.

Front office operations are most visible in an online government world. While the emphasis again is different, the basic functions have many similarities with their business counterparts. One particular area of interest that can be borrowed from the world of business is customer/constituent relationship management (CRM). Businesses use CRM to better understand the needs and preferences of their customers, and thereby tailor their services to these needs (i.e. a store discovering that flashlights should be placed next to Halloween costumes). Unlike the polls typically relied on by government agencies, CRM analyzes usage patterns and other factors to provide an objective view of citizen needs.

What makes this model so potent is its ability to tie disparate organizations or agencies into one common set of functions. This commonality enables information and application sharing across organizations in a comprehensive enterprise view. Now that we have established a model, let us explore its implementation.

Objectives and Benefits

Government's first step must be to set the goals and objectives for the electronic governance effort. Many organizations, commercial and otherwise, fall into the trap of incremental thinking when developing their electronic strategy. Lofty goal setting can guard against the tendency for conventional thinking and incremental gains—a sure prescription for failure in the zero-environment of the Internet ecology [3].

Grossly oversimplified, there are three primary areas government entities can pursue in setting electronic-strategy directions:

- It can increase revenues and optimize budget expenditures.
- It can reduce costs.
- It can improve constituent services.

Increasing Revenues

Every organization wants to increase revenues. The challenge is finding creative ways of increasing revenues that can provide funding to offer constituents enhanced services without additional taxation. Some areas where electronic data can assist include:

- **Selling information.** Data transmission such as high school records to colleges/universities for a fee is possible. Many states are selling or considering selling information over the Web, but issues such as privacy concerns can limit this.
- **Fee for service.** Arizona is charging user fees for some of the services it is offering on the Web. These fees are used to fund Web applications.
- **Improving collections.** Massachusetts is using the Web to simplify tax filings and payments. Using the Internet to provide better and more timely taxpayer information makes collection faster and easier. This encourages taxpayer compliance, increasing the odds that the returns are correct, and provides quicker access to tax funds.
- **Increasing compliance.** Using the Internet can simplify payment of parking fines and traffic tickets
- **Catching fraud.** Data warehouse applications can combine data from many sources to find fraudulent transactions, such as the same person filing multiple claims under different names, or duplicate/unmatched supplier disbursements.

Reducing Costs

Electronic media provides the government with the ability to dramatically reduce operating costs while improving its service to citizens. The state of Alaska provides a good example.

It implemented a Web and telephone interface that allows customers to renew automobile registrations without visiting the Department of Motor Vehicles. This resulted in cutting the state fulfillment cost from $7.75 to $0.91 and reducing citizen time from 2.5 hours (excluding travel) to less than three minutes (no travel). The State achieved a significant rise in citizen and employee satisfaction.

Alaska is reapplying this technology and process to its business license renewal department. While the states seem to be applying the Internet ecology more quickly than the federal government in some areas, clearly the benefits can be equally gained in areas of case management of entitlements, services such as those offered by the Veterans' Administration, and student loans. All of these functions are aggressively pursuing government use of the electronic media in the federal arena.

By applying best practices (such as the Software Engineering Institute's Capability Maturity Model® and effective IT management techniques, significant savings in IT operating costs can be obtained while simultaneously improving IT service levels. Outsourcing engagements, using the CMM Level 3 as a basis for management, have reduced operating costs 15 percent to 20 percent, reduced cycle time to up to 80 percent, and enhanced service levels raising customer satisfaction across the board.

Figure 3 displays the results of moving from CMM Level 1 to Level 3, based on an analysis of 1,300 projects developing 200,000 software lines of code. Achieving Level 3 provides the greatest benefit, both in deficit reduction and quality enhancement. When CMM processes are combined with the optimization of the government using the electronic media, the increase in available funding for developmental projects can be considerable for government entities. The benefits are significant and improve cost and quality, while reducing effort and time to market (cycle time). To survive in the fast paced world of e-business, performing at Level 3 or higher is not an option; it is a necessity.

Improving Constituent Services

There are endless ways to use the Internet and e-business concepts to enhance constituent services. The following are just some ideas drawn from the business world:

- Access to customized information is an obvious benefit of the Internet. For example, a retiree may get customized views of elderly services, while a youngster receives sports and education information. Non-English speakers may get information in their native language.
- Customer (constituent) self-service is used by businesses to lower customer support costs while increasing customer satisfaction. The government can benefit by transferring tasks to the constituents, who can work at their pace and schedule while reducing the time and inconvenience of performing the transaction. Some examples include allowing customers to file and research consumer complaints online, enabling citizens to inspect and correct personal government records, and providing such benefits as electronic tax filing.

These benefits are exciting, with huge potential return on investment. But there is a big difference between strategy and implementation. The quality of the implementation is as important as the quality of the technology. A government project in the electronic media is a big challenge, involving large applications that are difficult and complex to develop and roll out. The majority of Internet-related projects still have a negative return on investment, as witnessed by the performance of most web initiatives. These poor results, however, are not a reflection on e-business change management. Many years of large project management experience and $100 million-plus run rate of Internet projects can offer some lessons.

Managing Cross-Functional Projects

Successful e-business projects require a cross-disciplinary approach that includes business, technology, and creative components. The commercial world is quickly developing people highly skilled in the rigors of e-business development and rollout. Making use of this expertise is essential if government organizations are going to avoid costly mistakes and reinventing the wheel. Some requirements are:

- **Process Improvements:** E-business benefits cannot be achieved by attempting to automate existing processes. All successful projects begin with a blank sheet of paper. Their processes are redesigned from scratch before attempting to design and build systems.
- **Staffing:** Many companies are discovering that recruiting and retaining the skills needed to enter the world of e-business is costly and difficult. But numerous costly and specialized skills are needed only for a short duration, during development. The commercial world deals with these difficulties through outsourcing and the creative location of people. However, retaining a core of these exceptionally skilled employees is essential for maintenance purposes.
- **Project Risk Sharing:** Software projects are inherently costly and risky, with the buyers of services bearing the entire cost and risk of project overruns and failures. Consulting firms have devised new and creative ways to share development risk. Through outsourcing projects payments are linked to service level performance and guaranteed cost reductions or development projects include progress incentives. A new and growing area is fee for services, in which the consulting firm foots the bill for the development and rollout of an e-business application in exchange for a percentage of the fees or resulting cost savings.

Just as the rules have changed for the relationship between the consumer/citizen and the provider of goods and services,

Figure 3. *Quantifiable Business Benefit*

Quantifiable Business Benefit

CMM Level	Calendar Months	Level of Effort	Defects Shipped	Median Cost	Lowest Cost	Highest Cost
Level 1	30 Months	600 Person Months	61	$5.5M	$1.8M	$100+M
Level 2	18.5 Months	143 Person Months	12	$1.3M	$0.96M	$1.7M
Level 3	15 Months	80 Person Months	7	$0.73M	$0.52M	$0.93M

changes must be made in the relationship between the government and its suppliers. Many initiatives and organizations, such as the Industry Advisory Council, lead this beneficial maturation.

However, all parties to relationships in the Internet ecology must quickly become aware of the threats—both known and as yet developing—that will comprise the greatest challenge in the coming decade.

A Double-Edged Sword

The growing demand for access to more information, in greater and greater degrees of specificity, parallels increasingly virulent and violent cyber-attacks and cyber-crimes. Government and business customers expect providers to develop intimate relationships instantaneously, while guaranteeing privacy and security. Even as electronic commerce larceny carries serious repercussions, the dangers of this new human dimension focus on two areas: national threats to the country, and our lack of understanding or awareness of potential downsides to cyberspace. While tactics using firewalls, encryption, public key infrastructure, and other security measures are essential, we need to understand—at a deeply scientific level—the huge novel ecology we have created and entered.

Sen. Bob Bennett (R-Utah), at the October '99 Executive Leadership Conference in Richmond Va. attended by more than half of the federal chief information officers, pointed out that the Internet "... is a place. It is real. It brings trade and terrorism. And there are no oceans in the Web."

If you go to www.cybergeography.com, you will be able to view a beautiful and bewildering number of cyber-maps, showing the Internet from novel perspectives [4]. My favorite presents it in an abstract spider web of assorted colors, representing different countries. It reminds me of nothing so much as ganglions and neurons in the brain—the reds of Germany intertwined with the United Kingdom's lilac, U.S.' purples, and all the other colors of countries online. An example of a cybergeography map is shown in Figure 4.

Bennett's point underscores the lack of boundary dimension of the Internet, which brings not only any museum's masterpieces or your favorite chef's recipe, but also the threats of demented minds and hostile groups. We are now everyone's neighbor, but without some fundamentally protective human skills. The eye-to-eye contact we use to confirm honesty, and the handshakes, which communicate nervousness or deceit, are no longer there for us. We have removed the very heart of body knowledge, and operate purely on the basis of rational, logical thought. Unfortunately, we did not evolve that way, and therefore, cannot exercise judgment on the basis of comprehensive human understanding.

Neurophysiology over the past decade has made remarkable discoveries of both the essential role of emotions for effective decision making, and the seamless relationship between the body-state, and the perception of emotions. In his groundbreaking book, *Descartes' Error: Emotion, Reason, and the Human Brain*, Dr. Antonio R. Damasio proposes:

> "... Reason may not be as pure as most of us think it is or wish it were, that emotions and feelings may not be intruders in the bastion of reason at all: they may be enmeshed in its networks, for worse and for better.

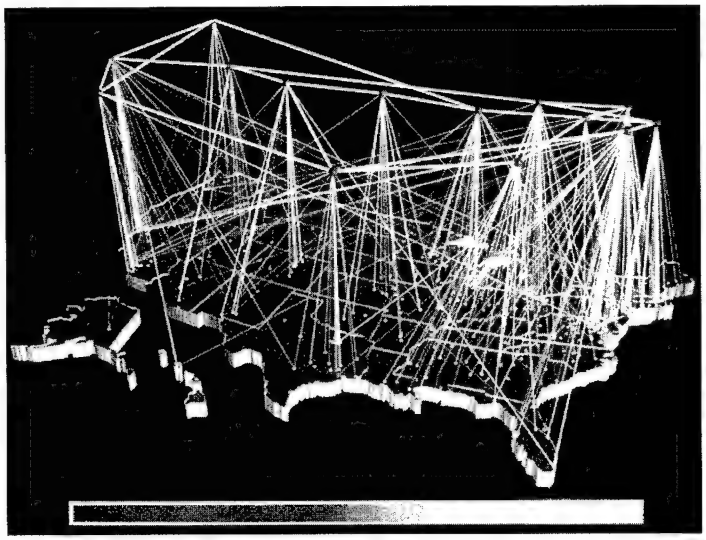


Figure 4. *Visualization Study of the NSFNET*

> The strategies of human reason probably did not develop, in either evolution or any single individual, without the guiding force of the mechanisms of biological regulation, of which emotion and feeling are notable expressions. Moreover, even after reasoning strategies become established in the formative years, their effective deployment probably depends, to a considerable extent, on a continued ability to experience feelings [5]."

To state a complex discussion in an overly simplified manner, he demonstrates that body-state, our basic hormonal/chemical signals, triggers what we call feelings—those feelings are central to effective decisions that contribute to survival. More specifically, all of us can recall the sense of unease when we feel deception, but cannot quite verbalize why we know we are being lied to. And lying, per se, requires language.

Robert Wright, in *The Moral Animal: Why We Are the Way We Are*, writes, "Language evolved as a way of manipulating people to your advantage ... cognition, the wellspring of language, is warped accordingly [6]."

In ecology devoid of the somatic wisdom of face-to-face interaction, the advantage goes to deceivers. Heightened awareness of this essential characteristic of the Internet dimension must be a fundamental element of all our interactions, both at the national and personal levels. The growing assault on industry and government sites is being met with escalating security procedures and tools—it is a seesaw balance of terror that is probably a never-ending exchange. On the personal level, though, we must grapple with a change none of our forebears could have even imagined.

In his book *Creativity*, Mihaly Csikszentmihalyi points out that evolution in the past millennia has been driven by cultural forces far more than biological forces. Great minds, like Jonas Salk and Edmund O. Wilson, have called this tendency metabiological or biocultural. We are changing ourselves, our cultures, and *directing evolution* faster than biology. What we have now is a new dimension in which to exist, and like all great dramatic changes in human evolution, it carries powerful positive and negative consequences. But it is real. It is a place. And now there are no distances between either our enemies or our friends.

The Promise of the Future

Great leaps forward in technology, like the car, electric power,

and the Internet, inevitably carry great benefits and usually unanticipated downsides. Governance by electronic media, like e-business, is here to stay. And in a decade's time the issues and challenges of this article will seem childlike and innocent; the benefits will seem unimaginative and lacking foresight. Clearly though, government will play an increasingly important role as President Clinton stated in his National Plan for Information Systems Protection (V.11):

> "The federal government does ... have an important role to play. This includes research and development efforts in the field of computer security, educating a corps of young computer scientists to help defend our federal cyber systems, and assisting the private sector as it creates defensive measures for its information technologies ... it is an essential undertaking that we must begin now, so that we can continue to enjoy the extraordinary opportunities of the Information Age and create the security we require for our prosperity and growth in the next century [7]."

As the thinkers and innovators of information technology, we in the field of software engineering owe our nation and ourselves a deep understanding of what it means to communicate, to decide, and to enter into relationships in the absence of body-knowledge. We must quickly bring the benefits of this new ecology to the realm of governance, taking advantage of the lessons learned in the private sector and looking to their leadership in some fields.

It must not be just a technological surge of understanding information security, though, but a paired commitment to understanding human decisions, feelings, and the seamless communication between our bodies and our brains. Only when we can dovetail these branches of communication theories will we truly feel secure in the Internet ecology.◆

Acknowledgements

Many thanks go to Brian Keane, CEO, Keane Inc., for his notes from the Florida Government Technology Conference, September 1999. Portions of this article were first discussed at my presentation to the U.S. Navy Symposium on Information Security for Chief Information Officiers, Brookings Institute, Washington, DC, in November 1999.

References

1. *BizReport.com Newsletter,* 1/11/2000, Issue 2. 2000, Vol. 3. Available at www.bizreport.com
2. Available at http://ecom.wharton.upenn.edu/news.html
3. Yeh, Ray, Ph.D. Pre-publication review draft, *Zero-Time Organizations,* publication in Fall 2000.
4. Cox, Dana and Patterson, Robert. *Visualization Study of the NSFNET from the NCSA,* 1992, www.cybergeography.com/atlas/geographic.html
5. Damasio, Antonio, Ph.D. *Descartes' Error: Emotion, Reason, and the Human Brain,* Avon Books (1994), p. xi.
6. Wright, Robert, *The Moral Animal: Why We Are the Way We Are,* Vintage Books (1994), p. 295.
7. The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0,* , 2000, p. ii.

The Dana Alliance for Brain Initiatives maintains a Web site at www.dana.org/brainweb, which is a neurosciences Internet *Best Bet* and a Lycos Top 5 percent site.

Additional Reading

The following books delve into human brain functions, consciousness, organizational evolution, and human social hierarchies. They are particularly germane to the issues discussed in this article.

The Feeling of What Happens: Body and Emotion in the Making of Consciousness by Antonio R. Damasio

Descartes' Error: Emotion, Reason, and the Human Brain by Antonio R. Damasio

The Mind of the Strategist: The Art of Japanese Business by Kenichi Ohmae

The Engine of Reason, the Seat of the Soul: A Philosophical Journey into the Brain by Paul M. Churchland

Built to Last: Successful Habits of Visionary Companies by James C. Collins and Jerry I. Porras

The Evolution of Progress: The End of Economic Growth and the Beginning of Human Transformation by C. Owen Paepke

The Moral Animal: Why We Are the Way We Are: The New Science of Evolutionary Psychology by Robert Wright

Creativity: Flow and the Psychology of Discovery and Invention by Mihaly Csikszentmihalyi

The Logic of Failure: Why Things Go Wrong and What We Can Do to Make Them Right translated by Dietrich Dorner

Managing to Have Fun by Matt Weinstein

The Face of Battle by John Keegan

A History of Warfare by John Keegan

Origins of the Sacred: The Ecstasies of Love and War by Dudley Young

Blood Rites: Origins and History of the Passions of War by Barbara Ehrenreich

Well Made in America: Lessons from Harley-Davidson on Being the Best by Peter C. Reid

About the Author

Nancy Lee Hutchin is the bid and proposal manager for Keane Federal System Inc. and has an international reputation for professional excellence, with 22 years experience. She has had more than 30 articles published and participated in six international conference program committees, including more than 20 presentations, numerous keynote speeches, and serving as track chairwoman. The 45-plus projects she has successfully concluded have covered change management, information strategy, business process reengineering, information engineering, strategic and implementation planning, and legacy system migration/enhancement. She was named International Woman of the Year for the United Kingdom's *Cambridge International Dictionary of Biography.* Hutchin also has been included in Marquise's *Who's Who in Finance and Industry, Who's Who of American Women, Who's Who in the World, Who's Who in Science and Engineering,* and *Who's Who in America.*

1410 Spring Hill Road, Suite 500
McLean, Va. 22102
Voice 703-848-7200
Fax 703-848-7607
E-mail: Nancy_L_Hutchin@Keane.com
Internet: www.keane.com

Continued from page 6, **About the Authors**

Ron Knode is the director for Information Assurance Solutions for Computer Sciences Corp (CSC). He leads an operation of nearly 350 information security engineers who serve both commercial and government clients with customized Information Risk Management Program solutions. He also supervises CSC's certified Trust Technology Assessment Program evaluation lab under the National Information Assurance Partnership. He is the author of more than a dozen articles on secure distributed information system architectures and multilevel database management systems.

Ronald B. Knode
Director, Information Assurance, CSC
7459A Candlewood Road
Hanover, Md. 21076
Voice: 410-691-6590
Fax: 410.684.2077
E-mail: rknode@csc.com

Mary Schanken is a Senior Computer Scientist with NSA who contributed to the development of numerous security documents. She served as government lead for the development of the SSE-CMM, and is implementing the SSE-CMM within the DoD. She is a Lead Assessor and Proficiency Test Grader for laboratories performing Common Criteria evaluations in the United States. She completed her Computer Science degree from the UMBC, and graduate studies at the UMUC, and the Naval War College.

National Security Agency
9800 Savage Rd Ste 6740
Ft. Meade, Md. 20755-6740
Voice: 410 854-4458
Fax: 410 854-6615
E-mail: schanken@nsa.gov

Coming Events 2000

October 15-19
Object Oriented Programming Systems Languages and Applications Conference (OOPSLA 2000)
www.acm.org/events

October 23-25
4th Symposium on Operating Systems Design and Implementation
www.usenix.org/events/osdi2000

October 30-31
3rd International Conference on Practical Aspects of Knowledge Management (PAKM 2000)
www.do.isst.fhg.de/workflow/events/index_e.html

November 10
Infomation Outlook 2000 (Australian Computer Society)
www.acs.org.au/act/events/io2000/index.html

November 16-17
ACM Conference on Universal Usability
www.acm.org/sigchi/cuu

December 4-7
International Conference on Power System Technology
www.ee.uwa.edu.au/~aips/powercon

December 11-13
Global Development Network Conference
www.gdnet.org

April 29-May 3, 2001
Software Technology Conference 2001
www.stc-online.org

The Survivability Imperative: Protecting Critical Systems, continued from page 15, **About the Authors**

Robert Ellison, Ph.D. is a Senior Member of the Technical Staff in the SEI Networked Systems Survivability Program. His research interests include system survivability and architectural patterns and styles for security architectures. He has a doctorate in Mathematics from Purdue University and is a member of the ACM and IEEE Computer Society.

Nancy Mead, Ph.D. is senior member of the technical staff in the SEI Networked Survivable Systems Program, and a faculty member in software engineering, Carnegie Mellon University. She is involved in the study of survivable systems requirements and architectures, and the development of professional infrastructure for software engineers. Prior to joining the SEI, Mead was a senior technical staff member at IBM Federal Systems, where she spent most of her career in development and management of large real-time systems. She also worked in IBM's software engineering technology area, and managed IBM Federal Systems' software engineering education department.

Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213

Dr. Thomas Longstaff is senior member of the technical staff at the Software Engineering Institute and currently manages research and development in Survivable Network Technology for the Networked Systems Survivability Program. He is a member of CERT® Coordination Center and conducts analysis of vulnerability and security incidents and methods for assessing survivability. Previously he was technical director at the Computer Incident Advisory Capability at Lawrence Livermore National Laboratory, Livermore, Calif.

Richard Linger is a senior member of the technical staff at the Software Engineering Institute's CERT® Coordination Center at Carnegie Mellon University. He teaches at the CMU H.J. Heinz School of Public Policy and Management. While at IBM, he founded and managed the IBM Cleanroom Software Technology Center. Linger has published three software engineering textbooks and more than 50 articles. He holds a bachelor's degree in electrical engineering from Duke University. He is member of the IEEE, ACM, the National Software Council, and vice-president of the Center for National Software Studies.

Avoid Self-Inflicted Wounds in Applying CMM to ATP and Support

By David B. Putman
Hill Air Force Base

If you have ever found yourself thinking that the Capability Maturity Model (CMM®) does not apply to you, you are not alone. Unfortunately, you may not be aware that the source of the problem may not be the CMM. The cause generally goes back to the method the organization chose for implementing the CMM concept. Size and critical computer resources are classic examples of areas in which the organization may need to step out of the box in order to look at the underlying concept related to requirements implementation.

Exploring the Size Metric

Years ago someone in our organization defined the size of a project as source lines of code (SLOC). This became a size metric. The waivers for tracking size quickly followed; the rationale being, SLOC does not make sense when providing a maintenance level of support or designing hardware. This quickly led to more fuel for the fire as to why the CMM did not apply in numerous areas. Many failed to consider an alternative size metric. Those that developed alternative metrics, however, often failed to recognize that the alternative did indeed meet the concept of the size metric.

We eventually broadened the definition of the size metric so it could be applied to all projects. I recently explored the size concept with Will Hayes, senior member of the technical staff of the Software Engineering Institute (SEI). This discussion helped confirm that the present concept of the size metric should have been implemented when the Project Planning Key Process Area was originally addressed. The only problem was that parties were so busy arguing SLOC that they failed to see what was right in front of them.

One of the concepts in the CMM is to document the process used when preparing an estimate (i.e. capture the thought process, data, etc.). Documenting the estimating process reduces the dependency on expert opinions and improves the repeatability of the estimates. Comparing the actuals to the estimates helps improve the accuracy of the next estimates.

The CMM refers to size in relation to estimating the cost and schedule required to develop a product. With that concept in mind, a simple definition of cost and schedule can be defined as:

Cost = Size * Productivity in Dollars
Schedule = Size * Productivity in Days

Where,

Size = a measure or indicator of the amount of work to be performed in terms other than dollars or hours;
Productivity = a cost or schedule metric that indicates the rate at which the measurement of work can be performed.

As the product is decomposed into smaller elements and the organization better understands its capabilities, the equations may be expanded as shown below:

$Cost = (\Sigma S_X * P_{X \text{ in Dollars}}) * (1 + Percent\_Risk)$
$Schedule = (\Sigma S_X * P_{X \text{ in Days}}) * (1 + Percent\_Risk)$

Where,

S_X = Size of a particular task or part of the product;
P_X = The productivity to perform the task or develop that part of the product;
Percent Risk = a optional percentage that addresses such areas as:

— A range (e.g. from 0 to 0.25) that takes into account the team's learning curve, training, experience and motivation. For example, if the project is assigned to the top performers in the organization, the product may be completed as originally estimated; if the project is assigned to less experienced team members the project may take 25 percent longer to complete.
— A correction factor for the estimator's bias. In this example the estimate is dependent upon an expert's opinion. This correction factor recognizes that the time it would take the expert to complete the task may vary from the time it would take the typical employee to complete the task.
— Potential impacts resulting on dependencies on subcontractors, procurement, or other activities outside the organization's control. For example, many estimates will include a schedule buffer that takes into account the average time that it takes for the procure- ment of piece parts. Even though the average time has been taken into consideration, there is a risk associated with the fact that the parts may not be received in the average time frame.

The sections below explore using the size metric when preparing estimates for efforts related to developing and maintaining automatic test equipment (ATE) product. The sections are broken out in the following areas:

- Conceptual approach for estimating the cost for ATE Test Program Set (TPS) maintenance.
- Conceptual approach for estimating TPS development.
- Conceptual approach for estimating test station replacement and sustainment activities.

Estimating ATE TPS Maintenance Cost Conceptually

Applying the concept of size to maintenance activities is fairly easy, but the managers of ATE TPS software maintenance activities often look at the size metric from the wrong perspective. Maintenance estimates can be calculated using the following definitions:

Size = The number of maintenance tasks (analysis/ updates) that can be anticipated over a specified time frame (e.g. a quarter or a year). A review of historical data and trends can quickly result in a size estimate.

$Productivity_{\text{ in Dollars}}$ = The average cost per maintenance task.

$Productivity_{\text{ in Days}}$ = The average cycle time per maintenance task.

The necessary manpower to support the anticipated workload can be easily calculated once cost and schedule information has been estimated. Using the definition of size identified above, the size metric can easily be tracked. Examples of items related to size that could be tracked include:

- The number of maintenance tasks received each month.
- The number of maintenance tasks closed each month.

- The number of maintenance tasks open at the time of the monthly snapshot.
- The number of maintenance tasks in a work stoppage condition (i.e. the work stoppage is out of the control of the organization) at the time of the monthly snapshot.
- The average number of maintenance tasks per employee at the time of the monthly snapshot.

The workload level may have an impact on average cost and schedule. Many ATE customers will fund for a guaranteed level of maintenance support to cover a specific time frame. In this situation the average cost or schedule (cycle time) may be highly dependent upon the level of the workload in comparison to the guaranteed level of support. Figure 1 uses the concept of the economic supply and demand curves to represent the maintenance workload.

The curves shown in Figure 1 demonstrate that if the customer sends the team one task after funding for a guaranteed support level of $1 million then the cost per task is $1 million. The average cost per task decreases as more tasks are received until the average cost per task stabilizes when the team is fully loaded with work.

On the left side of the chart the average cycle time per task may start out higher than necessary due to the employees' concern about their future. On this side of the chart the employees may feel that they are faced with the dilemma of working themselves out of a job vs. *nursing* the project. This dilemma may lead to morale issues even though the team may be fully funded for the current time frame.

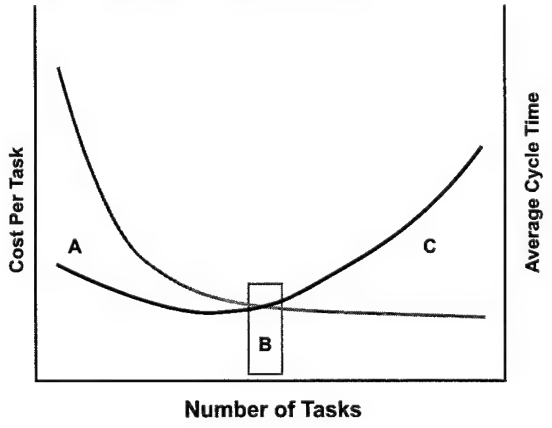
The average cycle time per task in Figure 1 will start to increase as resource limitations (manpower, equipment availability, etc.) start impacting the workload.

The optimum point for both cost and schedule occurs in the chart where the two lines cross on the graph (point B). Changes in the data must be well understood to determine whether the process is getting better or worse, or if the level of the workload is causing a shift along the curve. Process changes will raise or lower the curve. Workload changes (e.g. the number of tasks received) may cause a shift along the curve to the right or the left. Other workload changes, such as changes to the average complexity of the workload, may raise or lower the curve.

Estimating TPS Development Conceptually

In the early 1980s, I was given a cookbook formula for estimating TPS development efforts. This formula was developed in the '70s and worked well for circuit boards that contained small-, medium-, and some large-scale integration circuits. The formula was based upon the total number of integrated circuit (IC) pins in reference to the total number of input and output pins on the circuit card. The original formula did not work well as the integrated circuits became more complex. However, a variation of this original concept may work very well for estimating the size of the work to be performed for developing TPS.

Figure 1. *Cost vs. schedule for maintenance tasks*



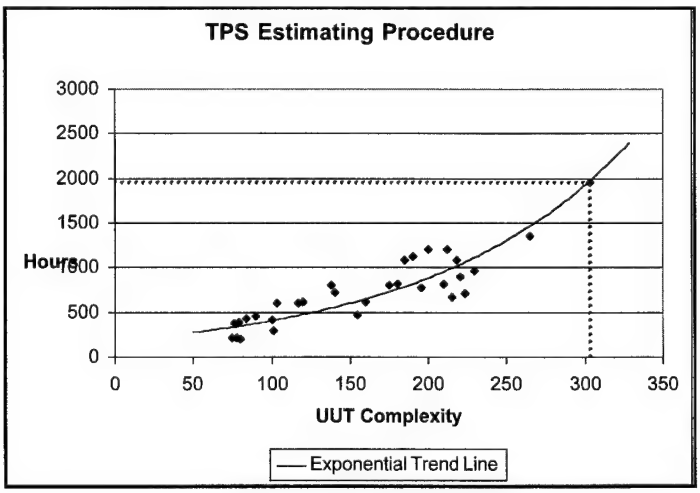
Component	Quantity	Weight	Rough Complexity
Small-, medium-scale integration	14 *	1 =	14
Counters, shift registers, etc.	8 *	2 =	16
Memory devices (programmable (array logic, read-only, random access ...).	16 *	4 =	64
Communication devices (universal asynchronous receiver transmitter, RS-232, IEEE-488, serial, parallel...)	4 *	15 =	60
16 bit microprocessors, micro-controllers, ...	1 *	75 =	75
32 bit microprocessors	0 *	100 =	0
Testability = [(quantity of ICs) * (20 pins/IC avg.) / (Total number of input/ output pins)] **2	= [(43*20)/100]**2		74
		TOTAL Complexity =	303

Table 1. *Example of a method to calculate a numerical complexity value*

Assigning a weighting factor to the various IC families can enable the project lead to calculate a number representing the complexity of the circuit card. It may also be possible to estimate the testability of the circuit card by comparing the number of input and output pins to other known parameters on the unit under test (UUT). Table 1 gives an example of how the complexity of the circuit card might be estimated in determining the amount of effort necessary to develop the TPS software. This example does not include developing component models for automatic test program generator simulators, interface test adapter (ITA) fabrication and other TPS development tasks that also need to be included in the final estimate.

Taking advantage of historical data, an organization can explore the weighing concepts discussed above in an effort to develop a reasonable correlation between the UUT complexity

Figure 2. *Example of plotting the correlation between complexity and cost*



Software Description	No. of Functions	Time per Function	Total Time (in hours)
Digital multi-meter software drivers (type of measurement, scale, filter, front/rear ...)	5 *	30 =	150
Timer/counter (type of measurement, scale, impedance ...)	5 *	30 =	150
Power supply drivers: five identical supplies providing +/- 20 VDC, 10 ADC power supplies (voltage, current)	2 *	20 =	200
Station self test (enter No. of tests) *[requirement is to ... such as test each stimulus and measurement at high-scale, low-scale, and mid-range]*	57 *	15 =	855
		TOTAL Labor Hours =	1355

Table 2. *Way of documenting process to estimate labor for the test station software*

diagram in Figure 2 shows an example of correlating the complexity to the effort. Spreadsheets, such as Excel, can calculate a variety of trend lines so that the user can find the best fit to the data. Using the graph shown in Figure 2, the cost to develop the TPS code for the example in Table 1 is $Cost_{in\ Hours} = 2.07\ e^{(0.0074*303)} \sim 1950$ hours of labor.

The cost of the ITA design, parts, and fabrication can be calculated using a table similar in nature to Table 1 but designed to meet the needs of the ITA estimates (see also section 2.3).

Estimating Test Station Replacement and Sustainment Activities Conceptually

Refurbishing or replacing the test stations involves similar types of work as developing a TPS from scratch. The activities include the design, the purchase of equipment and piece parts, the fabrication, and the development of software drivers, station self tests, and other software applications (e.g. test executives, post processors, program debuggers, TPS analysis applications, etc.).

Table 2 shows an example of how the software costs may be estimated. An example of estimating the hardware costs is shown in Table 3. Most ATE leads are very familiar with preparing a cost breakdown as shown in Table 3 for the hardware costs, but the similar practice for the software costs as shown in Table 2 does not seem to be as common. A similar table could also be developed to document the estimated fabrication costs of the items such as the cables, installing the instruments into the station, installing the cooling fans, etc.

Exploring Concepts Behind Critical Computer Resources

A discussion on risks is warranted before exploring the CMM concept for managing critical computer resources. From a simplified viewpoint risks can be grouped into two areas:

- Risks that may impact the team's ability to develop the product.
- Risks that may impact the product's ability to meet the performance requirements.

From a pure software viewpoint the critical computer resources (CCR) are the risks that may impact the product's ability to meet its performance specification. TPS developers and maintainers have been quick to point out that CCR is not applicable (or rarely applicable) in the ATE environment. Removing the focus on the word *computer* reveals that the concept of managing critical resources is applicable in the ATE environment.

Hardware Description	Quantity	Estimated Cost	Total Cost
Digital multi-meter	1 *	$2,500 =	$2,500
Timer/counter	1 *	$2,500 =	$2,500
DC power supplies	5 *	$1,000 =	$5,000
Oscilloscope	1 *	$15,000 =	$15,000
Wave form analyzer	1 *	$8,500 =	$8,500
IBM-compatible PC system (computer, monitor, keyboard...)	1 *	$5,000 =	$5,000
Piece parts (mating connectors, pre-fabricated cables, power strips, fans ... *this should be done at a reasonable level in an itemized format)*		$8,250 =	$8,250
			TOTAL Equipment Cost = $46,750

Table 3. *Way of documenting process to estimate cost of the test station hardware*

Tables 4 and 5 show two of the formats that an organization may choose for assigning a risk factor (R_F) to each potential risk. These tables assign a probability of occurrence and a severity to each of the risks identified. The tables also provide a method for determining a R_F that relates to the action required for each risk. The R_Fs used in Table 6 are based upon the R_Fs identified in Table 5 and assume that the organization has defined the actions as:

R_F = 1: No follow on action is required.
R_F = 2: The risks will be monitored and the probability and severity updated when necessary.
R_F = 3: A risk mitigation strategy will be developed.

By categorizing of the risks as development and performance risks, simple check sheets can be developed that will help in identifying and tracking them. For example, the left column of Table 6 could be used as a boilerplate or check sheet for TPS development risk management activities. It is highly probable that the

Table 4. $R_F = P * S$

<=100%	5	5	10	15	20	25
<80%	4	4	8	12	16	20
<60%	3	3	6	9	12	15
<40%	2	2	4	6	8	10
<20%	1	1	2	3	4	5
Probability		1	2	3	4	5
		Low		Med		High
		Severity				

Table 5. R_F = *the value identified in the cell*

<=100%	1	2	3	3	3
<80%	1	1	2	3	3
<60%	1	1	2	3	3
<40%	1	1	2	2	3
<20%	1	1	1	2	2
Probability	Low		Med		High
	Severity				

Table 6. *TPS Performance Risks*

Risk	P	S	R_F	Action
Product Development Risks				
Critical Personnel: Key personnel, critical to the successful completion of the product, may leave the organization.	1	5	2	This concern will be monitored
Support Environment: The organization may be unable to provide the necessary support environment necessary for the development of the product (e.g. computer access, software application tools, testing and integration environment.).	4	5	3	**Mitigation Plan:** The success of the project is highly dependent upon the availability of the ATE for integrating and testing the TPS. The owners of the ATE (production shop) have signed the SOW showing their intent to support the development to the maximum extent possible. However, production items take precedence over developmental TPSs. This risk has been identified in the proposal and any cost and schedule impacts will be negotiated with the customer if sufficient ATE is not available.
Procurement of Piece Parts: The organization may be unable to get the piece part hardware in a timely manner.	3	5	3	**Mitigation Plan:** The development schedules for the TPSs were expanded to allow xx days for the procurement of the parts necessary for the ITAs. The xx day schedule extension for each TPS was based upon the historic average of the number of days we have waited for the delivery of parts.
Product Performance Risks = Resources critical to the Performance of the product				
Available RAM: The amount of RAM available in the CPU may impact the successful operation of the product.	1	1	1	Automated segmentation utilities are used to assure the program segments do not exceed 80 percent of the available RAM.
Throughput: The CPU throughput (speed, run-time, etc.) may impact the successful operation of the product.	1	1	1	N/A:
Available Disk Space: The amount of disk space may impact the successful operation of the product.	1	1	1	N/A: The ATE has sufficient disk space to host approximately xx TPSs. Unused TPSs are deleted by the ATE operator (when necessary) to free up disk space; these TPSs can be quickly reloaded should they be needed in the future.
Other Test Station Resources (Power)				
Unit Under Test (UUT Power: The ATE may be unable to meet the power requirements for the UUTs (e.g. No. of DC/AC power supplies, voltage levels, current requirements, ripple, etc.).	5	4	3	**Mitigation Plan:** Full load testing of the gun controller circuit card requires providing 28 VDC at 50 ADC to the gun firing . circuitry. The power supplies in the ATE cannot provide this requirement. Two options have been identified in the proposal (1) use an external power supply to provide the power or (2) do not test the circuit under full load. The first option raises the development costs and increases the shops support costs (calibration, repair and spares), the second option has a risk of not catching a small percentage of the darlington transistor failures. We will implement the solution that is negotiated with the customer.
Cooling: The ATE may be unable to provide the cooling necessary for testing the UUT.	2	1	1	N/A: There is a small risk that certain UUTs may need cooling that has not been identified in the test specifications. If necessary, small fans can be installed in the ITA.
Other Test Station Resources (Input Signals)				
Waveforms: The ATE may be unable to provide the necessary waveforms to meet the requirements of the UUTs (e.g. number of signals, frequency, amplitude, shape, etc.).	2	3	2	Monitor: Ancillary equipment of additional hardware design may be necessary.
DC reference: The ATE may be unable to provide the necessary DC references to meet the requirements of the UUTs (e.g. number of signals, voltage level, precision).	2	3	2	Monitor: Ancillary equipment of additional hardware design may be necessary.
Pneumatic Inputs : The ATE may be unable to provide other necessary input signals.	5	5	3	The Sample Data Assembly requires a special timing signal in order to function properly. This timing signal is generated from an on-board clock signal. The proposal includes the cost and schedule necessary to design and instal this function into the interface test adapter.
Other Test Station Resources (Measurement System)				
AC Voltage Measurements (range, resolution, accuracy, etc.)				N/A: Calculations can be made during the development of the TPS to convert Peak-to-Peak values stated in the specifications to true RMS measurement readings.

ment risk management activities. It is highly probable that the risks shown in Table 3 were considered during the development of the TPS proposals, but often the results of this thought process were not always documented.

In looking at TPS maintenance activities, the problem analysis may reveal that one of the TPS Performance Risks identified in Table 6 is the cause of the identified problem. However, with the emphasis switched from TPS development to TPS maintenance, a performance problem is no longer a risk but an issue that must be addressed. In this case the organization may chose to condense all individual ATE resources identified in Table 6 to a single entry such as:

Risk: The engineering analysis may reveal that the equipment in the ATE and ITA may not meet the performance requirements of the UUT.

Mitigation: None. The engineering analysis and recommendation report sent to the customer will identify the performance issue and when possible make recommendations as to how the performance problem can be corrected.

Conclusion

The original intent of this paper was to show ways that the CMM could be applied in the area of supporting automatic test programs. TIS has gone a step farther by removing the software emphasis in TIS policy and guiding documentation; this enables us to apply the CMM concept to hardware engineering as well as software engineering. Hopefully this paper will help others who are struggling with CMM implementation issues to step out of self-perceived boundaries and to further explore the project man-

About the Author

David B. Putman is the Chief of the Operational Flight Program branch in the Technology and Industrial Support Directorate, Software Engineering Division at Hill Air Force Base, Utah. He has more than 21 years experience in ATE, two years with Hughes Aircraft, and more than 19 years with the Air Force. During his involvement with ATE, he was the senior engineer within the Avionics Software Support Branch for nine years, and he supervised ATE engineering teams for two years. He supervised the F-16 OFP system design and integration test teams for one year, and he was the SEPG lead when OO-ALC was assessed at a CMM Level 5. He has a bachelor's degree in electrical engineering from the University of Utah and a master's degree in business administration from Utah State University.

OO-ALC/TISF
7278 Fourth Street
Hill AFB, Utah 84056
Voice: 801-777-4726
Fax: 801-777-8069
E-mail: david.putman@hill.af.mil

New CMMI℠ Product Integrates Processes

PITTSBURGH—Now organizations currently using different models for separately improving systems and software engineering can use one newly released model to improve, train and assess process more commonly and consistently.

CMMI-SE/SW Version 1.0, an integrated model for systems engineering and software engineering improvement, was released in August 2000. The integrated model is designed for product-development organizations to improve their engineering and project-management processes. It incorporates the best features of its source models: Capability Maturity Model for Software (SW-CMM®) V2.0 draft C and EIA/IS-731 Systems Engineering Capability Model (SECM).

This new model will enable organizations to build on previous investments in improvement based on the SW-CMM or the SECM, and at the same time to benefit from the standardization and commonality of the integrated model.

It was developed by the Capability Maturity Model Integration (CMMI℠) Project, a collaborative effort sponsored by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the National Defense Industrial Association with participation by government, industry, and the Software Engineering Institute.

Use of Electronic access to CMMI-SE/SW V1.0, and more information about the CMMI product suite, are available at www.sei.cmu.edu/cmmi or by calling SEI customer relations at 412-268-5800.

Bill Pollak, public relations coordinator
Software Engineering Institute
Office: 412-268-5656 Fax: 412-268-5758
CERT/CC media relations: 412-268-4793

Capability Maturity Model and CMM are registered in the U.S. Patent and Trademark Office. CMMI is a service mark of Carnegie Mellon University.

Give Us Your Information, Get a Subscription

Fill out and send us this form for a free subscription.

OO-ALC/TISE
5851 F AVE., BLDG. 849, RM. B-04
HILL AFB, UTAH 84056-5713
ATTN: HEATHER WINWARD
FAX: 801-777-5633 DSN: 777-5633
VOICE: 801-586-0095 DSN: 586-0095

Or use our online request form at **www.stsc.hill.af.mil**

FULL NAME:_____

RANK OR GRADE:_____

POSITION OR TITLE:_____

ORGANIZATION OR COMPANY:_____

ADDRESS:_____

_____

BASE OR CITY:_____ STATE:_____

ZIP:_____

VOICE: COMMERCIAL_____

DSN_____

FAX: COMMERCIAL_____

DSN_____

E-MAIL: _____@_____

BACK ISSUES MAY BE AVAILABLE

(PLEASE INDICATE THE MONTH(S) DESIRED.)

JUNE 1999_____MEASURES AND METRICS

AUGUST 1999_____SOFTWARE ACQUISITION

SEPTEMBER 1999_____DII COE

OCTOBER 1999_____BEST PRACTICES

NOVEMBER 1999_____CHANGE MANAGEMENT

DECEMBER 1999_____SOFTWARE EVOLUTION

FEBRUARY 2000_____RISK MANAGEMENT

MARCH 2000_____EDUCATION & TRAINING

APRIL 2000_____COST ESTIMATION

MAY 2000_____THE F-22

JUNE 2000_____PSP/TSP

JULY 2000_____CMMI

AUGUST 2000_____PROCESS IMPROVEMENT

SEPTEMBER 2000_____COTS

Three Cheers for Big Brother

"I returned and saw under the sun, that the race is not to the swift, nor the battle to the strong, neither yet bread to the wise, nor yet riches to men of understanding, nor yet favour to men of skill: but time and chance happeneth to them all." –Ecclesiastes

"Objective considerations of contemporary phenomena compel the conclusion that success or failure in competitive activities exhibits no tendency to be commensurate with innate capacity, but that a considerable element of the unpredictable must invariably be taken into account."
–George Orwell's "modern" translation of the above.

"One of you will be voted off the island and must leave immediately."
–host of *Survivor*

It was a bright cold day in March, and Windows clocks adjusted themselves for daylight savings time. Winston, his cell phone at his ear, slipped quickly through the security door of Bldg 101, though not quickly enough to drop off the screen of his GPS. The hallway smelt of silica and/or asbestos. At one end of it was an enormous color poster from Kinko's. It depicted an enormous face of a man of about 45, with a heavy black moustache and ruggedly handsome features. Winston turned on his computer. It was no use trying to log on to the network. Even at the best of times it was seldom working, and at present the Herbie virus shut it down most of the time. It was part of the security drive in preparation for Complacency Week.

Fortunately the surveillance camera above his cubicle and the recording devices were hard-wired to a remote location, for the doubleplusgood of Winston and the Party. His login screen was the same as the poster in the hall, BIG BROTHER NEEDS YOU . . . the caption beneath it scrolled. From his speakers emanated a digital voice reading out a list of how he was to spend his day, and how it should be billed. When the voice said, "Nice haircut, Winston," he waved at the two-way mirrored glass on the opposite wall. He felt strangely welcomed by his telescreen at work; it was far better than the one at home that lately had only shown him *reality*-based programming. He found it to be nothing more than a bunch of Proles fighting for attention. This morning he was welcomed to work by a streaming video of the weekend's parade. He had thought about going but it had been hot and he knew the edited version would be more efficient.

One of the majorettes caught his eye until he saw the pink sash identifying her as a member of the junior antivirus league. At the end of the parade the MC spoke about how things had improved since 1984. Now we had sharp razors and antibacterial soap. Besides, we had peace in our time. Instead of two-minutes-hate, we now had two-minutes-indifference. There seemed to be no color behind the speaker aside from the tremendous Big Brother posters.

His face gazed down from every commanding corner. There was one on the house-front immediately opposite. BIG BROTHER NEEDS YOU . . . TO TRY OUT FOR THE NEXT REALITY-BASED SHOW. The poster's dark eyes seemed to have dollar signs for pupils. Down at street level another poster, torn at one corner, flapped fitfully in the wind, alternately covering and uncovering the phrase IGNORANCE IS STRENGTH. In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a satellite, and darted away again with a curving flight. It was a film crew, snooping into people's windows. Privacy didn't matter. Only the Thought Police mattered. Winston checked for stubble real-time in his huge monitor.

—Matt Welker, Shim Enterprise Inc.

CROSSTALK / TISE
5851 F Avenue
Building 849, Room B04
Hill AFB, UT 84056-5713

PRSRT STD
U.S. POSTAGE PAID
Kansas City, MO
Permit 34